HELSINGIN KAUPPAKORKEAKOULU
Liiketoiminnan teknologian laitos

PK –YRITYKSEN TIETOTURVAN ANALYSOINTIMENETELMIEN VERTAILU
Case: SystemIntelligence Oy, tietoturvan analyysi

Tietojärjestelmätiede
Pro Gradu –tutkielma
Tuula Laukkarinen k21224
Kevät 2005

Hyväksytty laitoksen johtajan päätöksellä 18/5 2005

arvosanalla hyvä, 70p

Timo Saarinen KTT Matti Rossi KTT

HELSINGIN KAUPPAKORKEAKOULU
Tietojärjestelmätieteen pro gradu –tutkielma
Tuula Laukkarinen

TIIVISTELMÄ

24.4.2005

PK –YRITYKSEN TIETOTURVAN ANALYSOINTIMENETELMIEN VERTAILU
Case: SystemIntelligence Oy, tietoturvan analyysi

Tavoitteet

Tämän tutkielman tavoitteena oli vertailla kirjallisuudessa esitettyjä yrityksen tietoturvan analysointimenetelmiä ja löytää sellainen menetelmä, joka soveltuisi pk –yrityksen tietoturvatason määrittämiseen. Lisäksi tavoitteena oli soveltaa valittua menetelmää kohdeyritykseen, määritellä kohdeyrityksen tietoturvan taso, arvioida menetelmän soveltuvuutta sekä löytää kehityskohteita ja antaa suosituksia kyseisen yrityksen tietoturvatason nostamiseksi.

Tutkimusmenetelmät

Tutkielma muodostuu teoria- ja empiriaosasta. Teoriaosassa määriteltiin aluksi tietoturvaan ja riskeihin liittyvät käsitteet. Käsitteiden jälkeen esiteltiin kirjallisuuden pohjalta yleisimmin käytettyjä tietoturvan analysointimenetelmiä ja vertailtiin niitä. Koska vertailun tuloksena ei löytynyt sellaisenaan soveltuvaa menetelmää itse analyysin suorittamiseen, on työssä kehitetty esitellyistä menetelmistä yhdistelemällä uusi menetelmä, rikastaminen, jota on empiriaosassa sovellettu kohdeyritykseen.

Tulokset

Sovellettu analysointimenetelmä ei huomioinut kyselyyn vastanneiden henkilöiden erilaisten toimenkuvien vaikutusta heidän antamiinsa vastauksiin. Tämä johti vastausten hajontaan siten, että vain yksi tietoturvan osa-alue (toimintasuunnitelmat) täytti puhtaasti analyysin kriteerit. Kriteerejä jouduttiin laajentamaan, jotta tutkittavien osa-alueiden joukosta saatiin järkevä. Mallin toiminnan luotettavuuden arvioimiseksi tulisi menetelmää soveltaa useammassa yrityksessä.

Kohdeyrityksen kannalta laajennetuin kriteerein suoritettu analyysi johti toivottuun lopputulokseen ja merkittävimmät tietoturva-aukot voitiin paikantaa.

Kohdeyrityksen tulisi liiketoiminnan kasvun myötä kiinnittää enemmän huomiota henkilöstöturvallisuuteen sekä lisätä tietoturvakulttuurin merkitystä. Lisäksi kohdeyrityksen tulisi nimetä henkilö vastaamaan yrityksen hallinnollisesta tietoturvasta, sekä osoittaa resurssit hänen käyttöönsä.

Avainsanat: tietoturva, riski, tietoturvaketju, todennäköisyys

SISÄLLYSLUETTELO

1. JOHDANTO

1.1. Motivaatio

Tietoriskien merkitys yritysten jokapäiväisessä toiminnassa kasvaa jatkuvasti. Ennen salassapidettäviä asiakirjoja säilytettiin turvassa kassakaapissa, nyt sama aineisto on tietovälineissä, joiden suojauksesta ei ole riittävästi huolehdittu. Samanaikaisesti yhä suurempi osa yritysten rutiineista hoidetaan tietojärjestelmien avulla, minkä seurauksena yrityksen toiminnan kannalta tärkeitä tietoja säilytetään ja käsitellään sähköisessä muodossa. Rutiinien muuttuminen manuaalisista automaattisiksi on ollut omiaan heikentämään tietoturvallisuutta.

Informaation saanti on elintärkeää tämän päivän liiketoiminnassa. Päivittäiset toiminnot ja päätöksenteon tukeminen ovat alueita, joissa informaatiota tarvitaan. Oikeiden ihmisten pääsy oikeisiin tietoihin, oikeaan aikaan on yhä tärkeämpää kilpailuedun saavuttamiselle, tai jopa busineksessa pysymisen edellytys. Samoin olemassaolon edellytyksenä on yrityksen arkaluontoisen informaation pysyminen luottamuksellisena.

1.2. Tutkimusongelma ja tutkielman tavoitteet

Tämän tutkielman tutkimusongelmana on pk -yrityksen tietoturvan tason arviointi. Alan kirjallisuudessa on esitelty runsaasti erilaisia menetelmiä yksittäisen yrityksen tietoturvan tason analysoimiseksi. Tämän työn ongelmana on selvittää kirjallisuudessa esitettyjen menetelmien toimivuutta kyseisessä arvioinnissa ja löytää sellainen menetelmä, jonka avulla on mahdollista suorittaa arviointi, sekä löytää mahdollisia kehityskohteita.

Tämä työ muodostuu teoria- ja empiriaosasta. Teoriaosan tavoitteena on aluksi määritellä tietoturvaan ja riskeihin liittyvät käsitteet. Käsitteiden jälkeen tavoitteena on esitellä kirjallisuuden tuntemia menetelmiä pk -yrityksen tietoturvan tason määrittämiseksi, mitkä ovat arvioinnit kohteet ja miten arviointiprosessi etenee yrityksessä. Vaihtoehtoisten arviointimenetelmien esittelyn jälkeen tavoitteena on vertailla eri menetelmiä ja löytää, tai vaihtoehtoisesti eri menetelmiä yhdistellen kehittää sellainen työkalu, joka parhaiten soveltuisi pk -yrityksen tietoturvan arviointiin ja riskien määrittelyyn.

Empiriaosan tavoitteena on arvioida case –tutkimuksen avulla valittua menetelmää. Ensin esitellään kohteena oleva yritys ja sen erityispiirteet tietoturvan näkökulmasta. Yritysesittelyn jälkeen käydään läpi tietoturvan arviointiprosessi valittua menetelmää käyttäen ja arvioidaan menetelmän toimivuutta tietoturvan arviointityökaluna. Tavoitteena on arvioida miten hyvin valitun menetelmän avulla pystytään löytämään kohdeyrityksen tietoturvasta sellaiset osa-alueet, jotka kaipaavat tarkempaa tutkimista. Empiriaosan lopussa kirjoittajan tavoite on myös esittää suosituksia tietoturvan tason nostamiseksi kohdeyrityksessä sekä luoda pohjaa tietoturvapolitiikan laatimiselle.

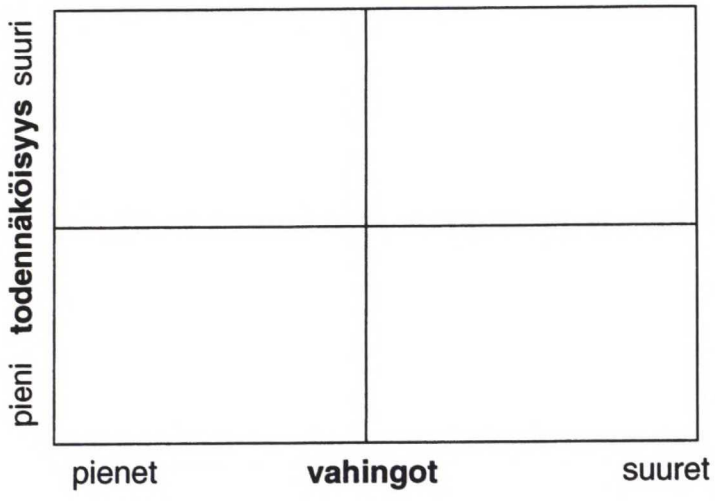
1.3. Käytetyt menetelmät

Työn teoriaosa pohjautuu kirjallisuustutkimukseen, IT-alan lehtiartikkeleihin, sekä aikaisempaan tutkimukseen tietoturvallisuuden alalta. Teoriaosassa esitellään viitekehyksenä Finnen (1996) kehittelemä CBISA –malli (Computer-Based Information Security Analysor). Finnen mallin lisäksi tietoturvakirjallisuudesta on etsitty muita menetelmiä, joita käytetään yleisesti

riskien analysoinnissa. Näitä menetelmiä on pyritty kuvaamaan siten, että lukijalle muodostuu kuva tekniikasta, jota kukin menetelmä edustaa.

Empiriaosa perustuu valittuun riskien arviointimenetelmään, jota sovelletaan kohdeyritykseen. Menetelmänä käytetään analyysin ensimmäisessä vaiheessa nelikenttäanalyysiin (kuva 1) perustuvaa kyselyä, joka pohjautuu soveltuvin osin teoriaosassa esiteltyyn Finnen CBISA –malliin. Nelikentän x -akselilla arvioidaan kunkin tietoturvatapahtuman yritykselle aiheuttamien vahinkojen suuruutta, mikäli tällainen tapahtuma realisoituisi. Nelikentän y -akselilla puolestaan arvioidaan kunkin tietoturvatapahtuman esiintymisen todennäköisyyttä. Empiriaosan pohjana oleva kysely on annettu täytettäväksi valitulle joukolle kohdeyrityksen henkilöstöä. Kyselyä on täydennetty tarvittaessa lisäkysymyksin.

Kuva 1. Nelikenttäanalyysi



Nelikenttäanalyysissa kyselyn vastaajat arvioivat kunkin tietoturvallisuuden osa-alueen sijoittamalla sen numeron nelikentän siihen lohkoon, joka parhaiten vastaa heidän mielikuvaansa tutkitun yrityksen tilanteesta.

1.4. Rajaukset

Tämän tutkielman ulkopuolelle on rajattu kohdeyrityksen oman kaupallisen tuotteen tietoturvallisuuden erityispiirteiden analysointi. Työ keskittyy kokonaisuudessaan tietoturvallisuuden hallinnolliseen näkökulmaan. Myöskin kohdeyrityksen tietoturvatason arviointi asiakkaiden ja yhteistyökumppaneiden näkökulmasta arvioituna on rajattu tämän työn ulkopuolelle.

2. TIETOTURVALLISUUS JA SEN ARVIOINTI

2.1. Määritelmät

2.1.1. Tietoturvallisuus ja haavoittuvuus

Tietoturvallisuudella tarkoitetaan kirjallisuudessa tietojen, järjestelmien ja palveluiden asianmukaista turvaamista sekä normaali- että poikkeusoloissa. Tietoturvallisuuden päämäärät ovat (Gollmann 1999, 59):

1) luottamuksellisuus (confidentiality)
2) eheys (integrity)
3) käytettävyys (availability).

Luottamuksellisuudella tarkoitetaan sitä, että data tai informaatio paljastetaan tai luovutetaan ainoastaan oikeutettujen henkilöiden, tahojen ja prosessien käyttöön.

Eheydellä tarkoitetaan datan ja informaation oikeellisuutta ja aitoutta. Eheyteen kuuluu myös ajantasaisuus, eli tieto ei saa olla vanhentunutta.

Käytettävyydellä tarkoitetaan sitä, että informaatio ja tietojärjestelmät ovat sekä ajallisesti, että muutoin tarvittavin tavoin käytettävissä ja saatavilla oikea-aikaisesti ja käyttökelpoisessa muodossa.

Haavoittuvuudella tarkoitetaan kaikkia niitä seikkoja, joiden vuoksi tietoja ei voi käyttää aiotulla tavalla. Tieto ei ole saatavilla, se on virheellistä, tai tallennettuja tietoja käytetään väärin (Ledell ym.1985, 11).

2.1.2. Riskikäsitteet

Riski on todennäköisyys, jolla jokin uhka toteutuu. Riski voi tarkoittaa myös epäedullisen tapahtuman arvioituja tai mitattuja seuraamuksia (Saarenpää ym.1997, 21).

Erilaiset tietoturvatapahtumat aiheuttavat eritasoisia seuraamuksia yrityksissä, jolloin riskien vaikutukset saattavat olla monitasoisia. Yrityksen kannalta yksittäisen tietoturvatapahtuman suurin riski on liikeriski. Liikeriskit ovat riskejä, jotka saattavat vaikuttaa pidemmällä aikavälillä koko liiketoiminnan tai yrityksen olemassaoloon (Tietojärjestelmien tarkastus ja valvonta ry 1997, 13).

Tietotekniikkariskejä ovat yksittäisten laitteiden, niiden komponenttien ja sovellusohjelmistojen toimimattomuuden tai virhetoimintojen aiheuttamat riskit. Ongelmat liittyvät yleensä tietotekniikan käytettävyyteen, eli laitteet ja ohjelmat eivät toimi tai ole hyödynnettävissä alkuperäisen tarkoituksensa

mukaisesti. (Saarenpää ym.1997, 37) Keskeinen hallintaväline on standardointi.

Systeemi- ja systeemiympäristöriskeillä tarkoitetaan yleensä tietoverkkojen, tietoliikenteen ja tietojenkäsittelyn toimivuuden ja luotettavuuden riskejä, esim. vuosi 2000 -ongelma (Saarenpää ym. 1997, 39).

Tietotekniikka- ja tietojenkäsittelyriippuvuuden riskit. Monet yritystoiminnan toiminnot ovat riippuvaisia tietojenkäsittelyn ja tietoliikenteen toimivuudesta. Toimintoja ei voida ilman suuria vaikeuksia ylläpitää tietojärjestelmien häiriötilanteissa.
Rikollisuusriskit. Tietotekniikka ja tietoverkot tarjoavat uusia ja tehokkaita välineitä rikolliseen toimintaan ja sen salaamiseen.

Tietoturvallisuutta voidaan luonnehtia useista muuttujista koostuvaksi kokonaisvaltaiseksi riskienhallintafunktioksi, eli kaikkien riskiä vähentävien toimenpiteiden ja niistä sekä arvioidusta toteutuneesta riskistä aiheutuneiden kustannusten minimoinnin muodostamaksi kokonaisuudeksi. Tietoturvallisuustoimenpiteissä pyritään saavuttamaan optimaalinen suhde tietoturvallisuusriskien ja tietoturvallisuustoimenpiteistä aiheutuvien kustannusten välillä. Optimointi edellyttää uhkien ja riskien taloudellista arvottamista optimoitavassa yhtälöryhmässä (Saarenpää ym. 1997, 49).

2.1.3. Riskien hallinta

Riskien hallinnalla (risk management) tarkoitetaan yrityksen kokonaisriskin hallintaa. Riskien hallinnan tavoitteena on löytää tasapaino riskin suuruuden ja suojaavien toimenpiteiden välillä (Hill & Smith 1995, 199). Riskien hallinta

muodostuu kolmesta osa-alueesta: (1) riskien tunnistaminen (risk identification), (2) riskianalyysi ja (3) riskien kontrollointi (Lane 1985, 112). Kaikkien riskien eliminointi on käytännössä mahdoton tehtävä, lisäksi äärettömän kallis, joten yritysten on pyrittävä löytämään tasapaino, jossa riskien hallinta on hyvässä suhteessa liiketoimintaan nähden.

Tietoturvariskeihin suhtautumiseen yritys voi valita kolmesta vaihtoehtoisesta politiikasta itselleen sopivimman.

a) Yritys voi valita riskien hyväksymisen, mikäli riskit eivät ole yrityksen toiminnan kannalta kestämättömät.
b) Riskien pienentäminen tasolle, jolla yritys katsoo voivansa vastata riskistä, on relevantti tapa käsitellä riskiä silloin kun käytettävissä on apuvälineitä ja tarvittavaa tekniikkaa.
c) Riskien siirtämisessä on käytetty perinteisesti lähinnä vakuutuksia. Monet vakuutusyhtiöt ovat kuitenkin viime vuosina kiristäneet ehtojaan kohonneiden korvauskustannusten johdosta, tai ovat kehittämässä täysin uudenlaisia, erityisesti tietoturvaa varten suunniteltuja vakuutuksia. Toinen, viime vuosien aikana voimakkaasti yleistynyt, tapa siirtää riskiä on ulkoistaminen (outsourcing). Monet yritykset ovat tänä päivänä ulkoistaneet esim. palvelimien ylläpidon sen sijaan, että panostaisivat oman laiteympäristönsä tietoturvallisuuteen esim. varmistuksin.

Lane (1985, 115) on kirjassaan maininnut lisäksi neljännen tavan suhtautua riskiin, nimittäin riskien välttämisen. Tällä hän tarkoittaa esim. sitä, että järjestelmään tehdään sellainen muutos, että riskin muodostava piirre liitännäisvaikutuksineen poistuu.

Valitun tietoturvapolitiikan tulee aina ulottua myös yrityksen ulkopuolelle siirtyvään tietoon, eli yhteistyökumppaneihin, alihankkijoihin ja etätyöläisiin. Etätyöntekijää, eli yrityksen ulkopuolelle siirtyvää tietoa uhkaa viisi pääaluetta: tietoa sisältävän laitteen varastaminen tai katoaminen, virukset, Internet-hyökkäykset koneeseen, verkossa liikkuvan tiedon salakuuntelu ja laiterikon aiheuttama tiedon menettäminen (Salminen 1997, 23).

Elbran (1992, 27) mukaan on olemassa neljä suhtautumistapaa tietoturvaan, mikäli unohdetaan kaikkein yleisin tapa, välinpitämättömyys:

1. Investoidaan kaikkiin mahdollisiin tietoturvalaitteisiin ja apuvälineisiin
2. Reagoidaan viimeisimpään "läheltä piti" uhkaan
3. Parsitaan aukot sitä mukaa, kun niitä ilmenee
4. Suoritetaan analyysi tietoturvariskien hallitsemiseksi

Tässä työssä keskitytään Elbran mallin kohdan 4 mukaiseen suhtautumistapaan, eli riskien hallintaan. Jotta riskejä voisi hallita, on kuitenkin ensin etsittävä menetelmä, jonka avulla mahdolliset riskit voidaan tunnistaa. Seuraavassa on esitetty menetelmiä riskien tunnistamiseksi ja arvioimiseksi.

2.2. Tietoturvan arviointimenetelmiä

Tietoturvan arvioinnilla (risk analysis, risk assesment) tarkoitetaan menetelmää, jossa arvioidaan riskit, joiden pohjalta voidaan implementoida toimenpiteet osa-alueille, joilla riskit ovat suurimmat ja / tai todennäköisimmät (Elbra 1992, 27).

Fisherin (1984, 80) mukaan riskianalyysin tarkoituksena on:

1. Auttaa riskitapahtumien identifioinnissa
2. Avustaa riskien arvonmäärityksessä
3. Auttaa riskien priorisoinnissa
4. Toimia pohjana kustannustehokkaalle tietoturvakontrollien asettamiselle

Käytännössä ei ole mahdollista eliminoida järkevästi kaikkia sellaisia tekijöitä, jotka muodostavat uhkan yrityksen tietoturvalle. Totaalikontrollien asettaminen tulisi todennäköisesti niin arvokkaaksi, että sen kustannukset saattaisivat ylittää niillä suojellun omaisuuden arvon. Riskianalyysin avulla voidaan erotella toiminnan kannalta kriittiset uhkatekijät, joiden poistamisella saavutetaan riittävä turvallisuustaso järkevillä kustannuksilla.

2.2.1. Arvottaminen

Yleisimmin kirjallisuudessa esitetty tapa arvioida tietoturvaa perustuu eri omaisuuserien kvantitatiiviseen arvottamiseen.

2.2.1.1. Alustavat toimenpiteet

Elbran (1992, 29) mukaan arvottamisen alustavat toimenpiteet ovat:

1. Määritellään arviointiprosessin rajat. Määritellään mitkä järjestelmät, laitteet, ohjelmat ym. sisällytetään prosessiin. Määritellään arvioidaanko kaikki riskit, vai esim. vain fyysiset riskit.
2. Varmistetaan, että kaikki osa-alueet on huomioituna: itse järjestelmä, data, laitteet, ohjelmat, menetelmät ja ihmiset.
3. Varmistetaan organisaatiorakenteen ymmärtäminen ja toimintojen dokumentointi.

4. Määritellään eri järjestelmille aikarajat, jonka jälkeen kyseisen järjestelmän saatavuus on yrityksen toiminnalle kriittinen, mikäli ko. järjestelmä ei olisi käytettävissä.
5. Listataan jo olemassa olevat menetelmät ja käytännöt tiedon turvaamiseksi.

Tämä kartoitusvaihe on itse analyysin onnistumisen kannalta kriittinen. Tässä vaiheessa kartoitetaan yrityksen nykyinen turvallisuustaso, jonka pohjalle lähdetään rakentamaan analyysin jälkeen uusia turvakontrolleja. Tässä vaiheessa huomiotta jäävät puutteet ja vahvuudet eivät yleensä tule tarkasteluun mukaan lainkaan, sillä analyysin seuraavat vaiheet perustuvat aina edellisen vaiheen tuloksiin (Freese 1988, 65).

2.2.1.2. Omaisuuserien arvon määrittäminen

Arvottamisen tarkoituksena on määritellä kaikki yrityksen tieto-omaisuus (assets) ja sen jälkeen se kustannus, joka yritykselle koituu mikäli kyseinen omaisuus on pois käytöstä tietyn ajan tai mikäli kyseinen omaisuus tuhoutuu lopullisesti.

Edellä mainittujen omaisuuserien arvottaminen on suhteellisen helppo tehtävä silloin kun kyseessä ovat laitteet tai valmisohjelmistot, sillä arvona voidaan käyttää niiden hankintahintaa. Ongelmalliseksi arvottaminen muuttuu itse tiedon osalta ja myös henkilöiden arvottaminen on parhaimmillaankin vain karkea arvio. Arvottamisessa tulisi ottaa huomioon myös se, että eri aikana jonkin tietyn tiedon tai henkilön arvo voi olla merkittävästi korkeampi kuin toisena aikana (esim. taloushallinnon järjestelmät kiireellisenä tilinpäätösaikana). Tietoturvariskien arvottamisessa tulisi aina käyttää suurinta mahdollista arvoa (Elbra 1992, 31).

2.2.1.3. Tietoturvauhkien tunnistaminen ja arvottaminen

Kun kaikki mahdolliset omaisuuserät on arvotettu, seuraava vaihe on tunnistaa mitä uhkia näihin eriin voi kohdistua. Uhkat voidaan jakaa fyysisiin (tulipalo, vesivahinko, virranjakelun keskeytyminen, varkaus jne) ja loogisiin (systeemivirhe, henkilökunnan tekemä virhe, virus jne). Uhkien tunnistamisen jälkeen asetetaan kullekin uhkakuvalle arvo:

Uhkatekijän arvo on sen tapahtumisen todennäköisyys (Elbra 1992, 33).

Uhkatekijöiden todennäköisyyden arviointi pohjautuu yleensä kvalitatiiviseen arvioon, joka perustuu arviointiin osallistuvien henkilöiden tuntemuksiin. Täsmällisen todennäköisyyden määrittäminen on näin epätodennäköistä, mutta sen sijaan tuloksena on usein luokittelu, jossa uhkan todennäköisyys on suuri, keskinkertainen tai pieni.

2.2.1.4. Riskin laskeminen

Arvottamisen menetelmässä voidaan riskin arvo laskea kertomalla kohdassa 2.2.1.2. määritelty omaisuuden arvo ja kohdassa 2.2.1.3. määritelty uhkatapahtuman todennäköisyys.

Riski = vahingon suuruus x tapahtuman todennäköisyys

2.2.1.5. Elbran muunnelma

Elbra on kirjassaan esittänyt laajennuksen edellä esitettyyn arvottamismenetelmään. Hänen mallissaan on uhkan todennäköisyyden käsitettä jatkettu määrittelemällä vahingon todennäköisyys, mikäli kyseinen uhkatekijä toteutuu.

Elbra onkin määritellyt riskin seuraavasti (Elbra 1992, 34):

> Riski = vahingon suuruus x vahingon todennäköisyys, mikäli uhkatekijä toteutuu x vahinkotapahtuman todennäköisyys

Edellä esitetty Elbran malli edustaa "täydellistä" mallia, johon käytännössä harvoin kuitenkaan päästään. Mallin heikkous on se, että kun kaikki tekijät mallissa on arvioitu "mielivaltaisesti", myös tulos on enemmän tai vähemmän mielivaltainen.

2.2.1.6. Courtneyn malli

Fisher on kirjassaan esitellyt vastaavan arvottamiseen perustuvan riskien määrittelymallin, Courtneyn mallin. Erona Elbran malliin on se, että Fisher on selvästi suuntautunut yksinkertaisempaan laskentatapaan ja toisaalta tuonut apuvälineitä todennäköisyyksien ja vahinkojen arvioimiseksi.

Fisher (1984, 84) esittelee riskin peruskaavaan R = P X C, jossa R on riski, P (probablility) todennäköisyys ja C (cost) kustannus.

Courtneyn mallissa todennäköisyys saa arvoja väliltä 1 –8 riippuen siitä, montako kertaa vuodessa kyseinen tapahtuma voi sattua ja tästä on johdettu kerroin (Loss Multiplier), joka kertoo tapahtuman todennäköisyyden vuodessa. Todennäköisyystaulukko on esitetty liitteessä 1.

Kustannusten määrittelyssä Fisher (1984, 85) painottaa, että on määriteltävä minkä tyyppisestä kustannuksesta missäkin tapauksessa on kyse, mikä sopii parhaiten kyseiseen vahinkotapahtumaan:

1. Kohteen fyysinen arvo
2. Kohteen korjauskustannukset
3. Kohteen korvaaminen uudella vastaavalla (sis. tilaus-, kuljetus- ja asennuskustannukset)
4. Kustannus, joka johtuu siitä että kohde ei ole käytettävissä (toimitusten myöhästyminen, yrityskuvan heikennys)
5. Varmistuksen kustannukset
6. Vakuutuksen kustannukset

Fisherin esittelemässä Courtneyn mallissa ei myöskään pyritä määrittelemään vahingon määrää tarkasti. Käytössä on subjektiivinen kustannus, joka on riittävän tarkka, jotta voidaan laskea riski R. Subjektiivisen kustannuksen taulukko on myöskin esitetty liitteessä 1.

Riskille saadaan siis arvo kertomalla keskenään "loss multiplier" ja subjektiivinen kustannus. Kyseisellä menetelmällä saadaan kunkin riskitekijän "vuosiarvo", mikä tulee muistaa verrattaessa riskiä esim. sen poistamiseen / pienentämiseen liittyviin kustannuksiin, jotka eivät välttämättä ole valmiina vuositason kustannuksina.

2.2.2. Kysymyssarjat

Kysymyssarjoja käyttämällä voidaan suhteellisen nopeasti luoda katsaus kysymyksiin vastanneiden henkilöiden käsityksiin yrityksen nykyisen tietoturvan tasosta. Kysymyssarjat eivät pyri riskien kvantitatiiviseen määrittelyyn, vaan vastaukset luokitellaan esim. luokkiin A – D, jossa A kuvastaa asian olevan kunnossa ja D toisena ääripäänä kuvastaa korkeaa riskiä.

Kysymyssarjojen ehdottomana valttina on niiden tekemisen nopeus. Myöskään tulosten analysointi ei vaadi monimutkaisia laskentamenetelmiä. Kysymyssarjoja käytetäänkin erityisesti avustamaan IT -henkilöstöä itse arvioimaan tietoturvallisuuden tasoa. Tulokset osoittavat riittävällä tarkkuudella ne tietoturvallisuuden osa-alueet, jotka kaipaavat lähempää tarkastelua (Fisher 1984, 43).

Tulosten tulkinnan helpottamiseksi eri alueiden kysymykset on ryhmitelty omiin kategorioihinsa. Esim. Fisher (1984, 43) on jakanut kysymykset kolmeen pääluokkaan: (1) fyysinen turvallisuus, (2) kontrollit, (3) toimintasuunnitelmat. Pääluokat on edelleen jaettu neljääntoista eri alaluokkaan.

2.2.3. Heuristiset menetelmät

Heuristisiksi menetelmiksi kutsutaan menetelmiä, jotka eivät perustu tosiasioihin, vaan tiedon jyväsiin. Nämä tiedon jyväset puolestaan perustuvat erilaisiin peukalosääntöihin ja aavistuksiin asioiden todellisesta tilasta. Heuristiset menetelmät antavat usein kuitenkin tyhjää paremman tuloksen tilanteessa, jossa tietoa ei ole käytettävissä (Lane 1985, 122).

Yksinkertainen esimerkki heuristisesta menetelmästä ovat erilaiset tarkistuslistat (checklists). Lisäksi aikaisempien kokemusten hyödyntäminen tulevaisuuden ennustamisessa on eräs tapa ennustaa riskien esiintymisen todennäköisyyttä. The exposure analysis methodology on eräs heuristinen menetelmä, joka luokittelee puolestaan yrityksen henkilöstön ammatin ja osaamisen suhteen. Tavoitteena on tunnistaa mahdolliset esim. henkilöstöön liittyvät tietoturvariskit (Lane 1985, 122).

2.2.4. Computer-Based Information Security Analysor

CBISA (Computer-Based Information Security Analysor) on Thomas Finnen (1976) kehittämä malli, jonka ajatuksena on helpottaa pienten ja keskisuurten yritysten tietoturvan tason analysointia. Itse malli on tarkoitettu päätöksenteon tukijärjestelmäksi (DSS) ja siten käytettäväksi sitä varten kehitetyn ohjelmiston ja tietokannan avulla.

CBISA –mallissa tietoturva on jaettu 12 alueeseen (modules), mikä helpottaa tämän erittäin laajan asian hahmottamista. Jokainen alue puolestaan muodostuu joukosta osa-alueita (submodules), joita mallissa on yhteensä 79 kappaletta (Finne 1976, 76-79).

1. Tietokoneturvallisuus (Computer security) -varmuuskopiointi, virustorjunta, tiedon salaus, salasanojen turvallisuus
2. Toiminnan turvallisuus (Operation security) –testaus, lokien seuranta
3. Varkauksilta suojautuminen (Protection against burglary) – kulunvalvonta, laitteistojen suojaaminen, laitteiden merkintä ja rekisteröinti
4. Tulipalolta suojautuminen (Protection against fire)
5. Vesivahingoilta suojautuminen (Protection against water damage)
6. Virranjakelun varmistaminen (Electricity distribution) – UPS, varavoima
7. Ulkoiset ja sisäiset uhkatekijät (Extern and internal threats)
8. Tietoliikenne (Communication) – modeemit, palomuurit
9. Toimintasuunnitelmat (Contingency planning) – onko olemassa?
10. Henkilöstöturvallisuus (Personnel security) – rekrytointi, vierailijat
11. Asenteet tietoturvaa kohtaan (Attitudes towards security issues) – onko kirjallinen policy?

12. Muut turvallisuusasiat (Various security questions) – paperitulosteiden käsittely

Tietoturvaketju (Information Security Chain, ISC) on kaikkien tietoturvaan vaikuttavien osa-alueiden muodostama ketju, joka ympäröi yritystä. Yrityksen tietoturva on juuri niin vahva kuin sen heikoin lenkki. Finnen (1976, 12) mukaan yrityksen tietoturvaketju muodostuu juuri edellä esitetyistä osa-alueista.

2.3. Menetelmien vertailu

Tutkielman empiriaosan toteuttamista varten on tässä kappaleessa tarkoitus valita tietoturvan arviointimenetelmä, joka parhaiten soveltuu käytettäväksi case –yrityksessä.

Arvottaminen (sekä sen muunnelmat Elbran malli ja Courtneyn malli) on menetelmänä erittäin perusteellinen ja kokonaisvaltainen menetelmä, joka etenee systemaattisesti vaihe vaiheelta. Menetelmä perustuu kvantitatiiviseen arvottamiseen, missä kuitenkin analyysia tekevien henkilöiden subjektiiviset käsitykset tietoturvauhkien todennäköisyyksistä antavat menetelmälle varsin epäluotettavan lopputuloksen. Arvottamalla saadut riskit saattavat olla liioiteltuja, sillä riskin tulontekijänä käytetään aina suurinta mahdollista arvoa kustannuksille. Menetelmä on monivaiheisuutensa vuoksi raskas toteuttaa, minkä lisäksi luotettavuutta heikentää se, että lopputulos on täysin riippuvainen aikaisemmissa vaiheissa tehdyistä ratkaisuista. Seikat, jotka ovat jääneet tarkastelun ulkopuolelle prosessin alkuvaiheessa, jäävät lopullisesti pois myös myöhäisemmistä vaiheista.

Elbran muunnelma poikkeaa perusarvottamisesta tarkkuudellaan. Elbra on jakanut riskin kaavan kolmeen tulontekijään, mutta lisätarkkuudella ei ole saavutettu lisää luotettavuutta lopputulokseen, sillä kolmas tulontekijä on arvioitu täysin subjektiivisin perustein.

Courtneyn malli on yksinkertainen kahteen edelliseen menetelmään verrattuna. Yksinkertaisuus on saavutettu helpottamalla riskitekijöiden subjektiivista arviointia valmiiden taulukoiden avulla. Courtneyn menetelmän avulla ei kuitenkaan päästä kovin luotettavaan riskin arviointiin, sillä taulukot on laadittu melko karkeiksi. Tämä malli soveltuu arvion mukaan melko hyvin samalla menetelmällä laskettujen riskien keskinäiseen vertailuun.

Kysymyssarjoja voidaan pitää nopeana tapana saada yleiskuva analysoitavan kohteen tietoturvan tasosta. Tulosten helppo analysointi on tulosta huolellisesti laaditusta kysymyssarjasta, joten itse kysymysten laadinta on työläin vaihe analyysista. Suurimpana heikkoutena tälle menetelmälle voidaan nähdä se, että se saattaa johtaa täysin puutteelliseen ja harhaanjohtavaan analyysiin, mikäli kysymykset eivät ole kattavia.

Heuristiset menetelmät ovat helppoja ja yksinkertaisia. Niiden käyttö on tosiasiassa perusteltua ainoastaan silloin, kun tarkkaa tietoa asioista ei ole olemassa. Heuristiset menetelmät eivät perustu mihinkään faktaan, vaan arvioihin tulevaisuudesta esim. menneisyyden perusteella. Sattuman vaikutus menetelmän antamiin tuloksiin saattaa olla erittäin merkittävä.

Finnen kehittämä CBISA –malli on puolestaan arvottamisen kaltainen kattavuudeltaan. Mallissa käydään läpi yrityksen koko tietoturvaketju, jolloin voidaan myös varmistua siitä, että kaikki osa-alueet ovat huomioituna. Menetelmä on kuitenkin varsin työläs, sillä kaikkien 79 tietoturvan osa-alueen

läpikäynti vaatii aikaa. Menetelmä on tarkoitettu käytettäväksi tietokoneavusteisesti, joten tehokas käyttö vaatii tarkoitukseen kehitetyn tietokannan ja ohjelmiston. Ehdottoman hyvänä puolena Finnen mallissa on se, että se antaa kvalitatiivisen ja konkreettisen tuloksen analyysista ja sen selkeä rakenne strukturoi hyvin koko tietoturvan käsitteen.

2.4. Käytettävän menetelmän valinta

Edellä esitetyn vertailun pohjalta voidaan tehdä johtopäätös, että jokaisesta käsitellystä menetelmästä löytyy toivottujen ominaisuuksien lisäksi joukko ei-toivottuja ominaisuuksia. Tämän johdosta mikään menetelmistä ei sellaisenaan tunnu sopivalta menetelmältä sovellettavaksi kohdeyrityksen tietoturva-analyysiin.

CBISA:n hyvät ominaisuudet vaikuttavat niin kiistattomilta, että sitä voidaan pitää hyvänä perusmallina ja lähtökohtana suoritettavalle analyysille. CBISA:n ehdottomasti huonoin puoli suoritettaessa analyysia ilman tarkoitukseen soveltuvaa tietokantaa, on sen vaatima suuri työmäärä. Suuri työmäärä johtuu siitä, että mallin mukaisesti tulisi käydä läpi kaikki 12 modulia ja niiden yhteensä 79 alakohtaa.

Courtneyn malli yksinkertaistettuna siten, että aiemmin esitettyjen kahdeksanportaisten arvotaulukoiden sijasta sekä riskin suuruudelle, että todennäköisyydelle annetaan arvo “pieni” tai “suuri” tarjoaa apuvälineen, jolla CBISA:n moduleista voidaan “suodattaa” pois ne, joiden riski vaikuttaa pieneltä tai epätodennäköiseltä tai muuten analysoitavan yrityksen kannalta merkityksettömältä. Näin jäljelle jäävät yrityksen tietoturvaketjusta ne modulit, joilla todella on merkitystä analysoitavan yrityksen kannalta. Jäljelle jäävien modulien analysointia voidaan jatkaa CBISA:n mukaisesti jakaen kulloinkin

käsittelyssä oleva moduli Finnen esittämiin osa-alueisiin. Kutsun tätä kaksivaiheista yksinkertaistetun Courtneyn mallin ja CBISA:n yhdistelmää jatkossa nimellä "Rikastaminen".

Taulukossa 1 on vertailtu esitettyjen menetelmien ominaisuuksia. Taulukon merkintä '+' tarkoittaa, että menetelmä pärjää vertailussa kyseisen ominaisuuden suhteen. Merkintä '-' puolestaan tarkoittaa, että menetelmä ei pärjää vertailussa kyseisen ominaisuuden suhteen.

Taulukko 1: Arviointimenetelmien vertailu, '+' = toivottu ominaisuus, ' –' = ei toivottu ominaisuus

Menetelmä/ ominaisuus	Arvotta-minen	Elbran malli	Courtney	Kysymys-sarjat	Heuristiset menetelmät	Finne CBISA	Rikasta-minen
Perusteellinen	+	+	+	+	-	+	+
Systemaattinen	+	+	+	+	-	+	+
Kokonaisvaltainen	+	+	+	+	-	+	+
Työläs	-	-	+	-	+	-	+
Monivaiheinen	-	-	-	+	+	+	+
Objektiivisuus	-	-	-	-	-	+ / -	+ / -
Antaa oikean kuvan	-	-	-	-	-	+	+

Edellä esitettyjen seikkojen ja vertailun lopputuloksena valitaan tässä työssä sovellettavaksi arviointimenetelmäksi rikastaminen. Rikastamisen etuna toiseksi parhaaseen menetelmään (Finnen CBISA) on se, että sen avulla pyritään löytämään jo analyysin ensimmäisessä vaiheessa ongelma-alueet, joiden tutkimiseen panostetaan seuraavassa vaiheessa.

3. TUTKIMUSMENETELMÄ

3.1. Tutkimusmenetelmän valinta

Tämän tutkielman empiriaosan tutkimusmenetelmäksi on valittu case - tutkimus. Tähän menetelmään on päädytty, koska tutkimuksessa on nimenomaisesti haluttu testata valitun tietoturvan analyisointimenetelmän soveltuvuutta aidossa yritysympäristössä. Koska tutkittavaa menetelmää ei ole käytetty muissa yrityksissä, ei sen tutkiminen käyttäen survey – menetelmää ollut mahdollista, vaan työ tehtiin case –tutkimuksena. Lisäksi analyysi suoritettiin valitun mallin mukaisesti kahdessa vaiheessa, mikä lisäsi menetelmän työmäärää. Suuren työmäärän vuoksi oli ensi vaiheessa mielekästä testata menetelmän soveltuvuutta vain yhdessä kohteessa.

3.2. Analyysin vaiheet

Ensimmäisessä vaiheessa analyysia suoritettiin itse "rikastaminen", eli karsittiin tutkittavan yrityksen tietoturvallisuuden osa-alueista pois ne alueet, joiden tarkempi analysointi ei ollut tarpeen. Ensimmäisen vaiheen rikastamisessa käytettiin apuna yksinkertaistettua Courtneyn mallia. Analyysi suoritettiin tekemällä kohdeyrityksen valituille henkilöille nelikenttämalliin perustuva kysely (liite 2). Kyselyyn vastaajien tuli sijoittaa Finnen mallin mukaiset 12 tietoturvallisuuden aluetta (tietoturvaketju) annettuun nelikenttään siihen kohtaan, joka heidän mielestään parhaiten kuvaa tilannetta kohdeyrityksessä. Lisäksi jokaiselta pyydettiin lyhyitä kommentteja perusteluksi kunkin alueen sijoittelusta. Saatujen vastausten perusteella valittiin toiseen vaiheeseen analyysiä ne alueet, joilla tietoturvariskit näyttivät yrityksen kannalta merkittäviltä.

Analyysin toinen vaihe keskittyy käymään Finnen mallin mukaisesti läpi toiseen vaiheeseen valittuja tietoturvamoduleja tarkemmalla tasolla. Toisen vaiheen analyysin tuloksena saatiin päätelmät siitä, ovatko kyseiset osa-alueet yrityksessä hoidettuna asianmukaisesti vai onko niissä merkittäviä tietoturva-aukkoja. Analyysin toisessa vaiheessa on käytetty apuna ensimmäisessä vaiheessa mukana olleille henkilöille tehtyjä lisäkysymyksiä ja haastatteluja.

3.3. Kohdeyrityksen valinta

Kohdeyrityksen valinnassa on määräävänä seikkana ollut yrityksen koko. Tutkimukseen on valittu pk –sektorin yritys, sillä suurissa yrityksissä tämän päivän tutkimustulosten mukaan tietoturva-asioihin on panostettu siinä määrin enemmän, että monien tässä työssä tutkittavien osa-alueiden on oletettu olevan kunnossa. Sen sijaan tutkimustulosten mukaan edelleen Suomessa pk –sektorilla on tietoturvallisuuteen panostettu erittäin vähän. Suurimmissa yrityksissä on yleensä olemassa keskitetty tietohallinto, jonka vastuulle tietoturva on määritelty. Pienemmissä yrityksissä ei usein ole erillistä tietohallintoa tai edes henkilöä, jolle tietoturva-asiat olisi vastuutettu.

Toisena seikkana kohdeyrityksen valinnassa on ollut toimiala. Tähän työhön on tarkoituksella valittu IT –alalla toimiva yritys, sillä se edustaa organisaatiota, jossa tarvittava osaaminen on olemassa, mutta asioiden jalkauttaminen on usein puutteellista.

4. CASE: SYSTEMINTELLIGENCE OY:N[1] TIETOTURVAN MÄÄRITYS

4.1. Kohdeyrityksen esittely ja kohderyhmän valinta

SystemIntelligence Oy on ohjelmisto- ja asiantuntijapalveluyritys, jonka 100% web-teknologiaan pohjautuva tuote auttaa asiakkaita kuvaamaan verkostoitumismallinsa sekä varmistamaan oikean tiedon olemassaolon, oikeaan aikaan, oikeassa paikassa.

Organisaatiorakenne

SystemIntelligence Oy on jaettu neljään yksikköön: New Business (myynti ja markkinointi), Product and Support (tuotekehitys, koulutus ja tukipalvelut), Customer Solutions (konsultointi ja koulutus) sekä Finance & Administration (talous, hallinto ja HR). Jokaisen yksikön vetäjänä toimii toimitusjohtajan alaisuudessa oleva johtaja. Yksiköiden toiminnallinen vastuu on toimitusjohtajalla.

SystemIntelligence Oy:n organisaatiorakenne on matala ja joustava. Yrityksessä työskentelee tällä hetkellä 24 henkilöä. Henkilöstön määrää on tarkoitus kasvattaa seuraavien vuosien aikana vastaamaan odotettavissa olevaa liiketoiminnan kasvua.

Päätöksenteko on SystemIntelligence Oy:ssä keskittynyt johtoryhmälle ja hallitukselle, päätettävästä asiasta riippuen. Johtoryhmän muodostavat edellä mainitut yksiköiden johtajat yhdessä toimitusjohtajan kanssa. Tietoturva-asioissa päätöksentekovaltaa ei ole täsmällisesti osoitettu kenellekään, vastuu lienee siis ensisijaisesti toimitusjohtajalla. Tosin hallinnollisen IT:n

[1] Yrityksen nimi on muutettu

osalta vastuuta on delegoitu talousjohtajalle, mutta yrityksen ydintoiminnan osalta tietoturva-asioita ei ole vastuutettu kenellekään erityisesti.

Markkinat ja asiakaskunta. SystemIntelligence Oy:n lähiajan tavoitteena on kansainvälistyminen. Asiakaskunta muodostuu tällä hetkellä meriteollisuuden, metsäteollisuuden, energia-alan ja julkisen sektorin organisaatiosta sekä konsulttiyrityksistä.

Kyselyn kohderyhmä määriteltiin käyttäen hyväksi yrityksen sisältä saatua informaatiota. Kyselylomake saatteen kera toimitettiin yrityksen Office Managerille, joka määritteli yrityksestä 4-5 toimenkuvaltaan kyselyyn sopivaa henkilöä. Määritellyistä henkilöistä Office Manager itse oli yksi, sillä hänen toimenkuvansa edustaa yrityksessä hallinnollista osaa, joka on tähän tutkimukseen valittu näkökulma. Muut tutkimukseen valitut henkilöt olivat sellaisia, joiden toimenkuvaan on kuulunut tai kuuluu tietoturvaan liittyvät asiat, kuten varmuuskopiointi, palomuurit ja palvelimien ylläpito. Vastauksia kyselyyn saatiin yhteensä kolme kappaletta, yksi Office Managerilta, yksi Product Architectilta ja kolmas Software Engineerilta. Product Architect on henkilö, joka vastaa yrityksen oman tuotteen kehittämisestä ja siten myös sen turvallisuudesta. Software Engineerin vastuulle taas kuuluu tällä hetkellä yrityksen palomuuri, virusturva, sekä yrityksen oman tuotteen pääkäyttäjätunnusten hallinnointi. Vaikka kyselyn laajuus ei kappalemääräisesti ollut kovin suuri, vastasi se kuitenkin melko hyvin kohdeyrityksen näkemystä tietoturvan tasosta, sillä tutkimukseen osallistuneiden määrä oli kuitenkin yli kymmenen prosenttia koko yrityksen henkilökunnan määrästä.

4.2. Analyysin ensimmäinen vaihe, nelikenttä

Palautuneiden vastausten (liite 3) käsittely aloitettiin käymällä läpi kaikki Finnen mallin mukaiset osa-alueet ja tarkastelemalla mihin kohtaan nelikenttää kukin vastaaja on kunkin osa-alueen sijoittanut. Tässä vaiheessa on kuvattu teorian valossa kyseinen osa-alue, sekä käyty läpi kunkin vastaajan mahdolliset perustelut tai kommentit kyseisen osa-alueen sijoitteluun liittyen. Vasta seuraavassa vaiheessa on etsitty yhteisiä tekijöitä saadulle kolmelle vastaukselle. Tavoitteena on ollut löytää joitakin tietoturvan osa-alueita, jotka kaikki kolme tai ainakin kaksi kolmesta vastaajasta mieltää joko korkean todennäköisyyden omaaviksi alueiksi, tai kyseisen tietoturvatapahtuman kustannukset on arvioitu suuriksi.

4.2.1. Tietokoneturvallisuus

Finnen mallin mukaisesti tietokoneturvallisuus keskittyy käsittelemään varmuuskopiointia, laitteiden elinkaaren hallintaa, virustorjuntaa, datan kryptausta, ja salasanoja.

Tietokoneturvallisuuteen liittyvien tekijöiden suhteen nelikenttäkyselyn tulos osoittaa, että yhden vastaajan mielestä tietokoneturvallisuusriski SystemIntelligence Oy:ssä on suuri sekä kustannuksiltaan, että todennäköisyydeltään. Yksi vastaaja on sijoittanut tietokoneturvallisuuden molempien tekijöiden suhteen alueelle ”pieni”, mutta aivan ylänurkkaan. Kolmannessa vastauksessa kyseisen tietoturvatapahtuman todennäköisyys on merkittävän suuri, mutta kustannukset arvioitu pieniksi.

Saatujen vastausten keskiarvona tietokoneturvallisuus sijoittuu nelikentän vasempaan ylälohkoon, jossa vahingon todennäköisyys on suuri ja kustannukset pienet.

Yhteenvetona vastausten perusteluista voidaan todeta, että salasanojen käytössä olisi kehittämisen varaa, kuten myös työasemilla sijaitsevien tietojen varmuuskopioinnissa. Yrityksen kaupallinen tuote, joka luonnollisesti on toiminnan kulmakivi, sijaitsee ulkoistetulla palvelimella, jonka tietojen varmuuskopioinnista huolehditaan päivittäin palveluntarjoajan toimesta.

4.2.2. Toiminnan turvallisuus

Toiminnan turvallisuudella tarkoitetaan Finnen mallin mukaisesti menetelmiä uusien ohjelmistojen tai ohjelmistoversioiden käyttöönottamiseksi, käyttäjätunnusten käyttöä, lokitietojen seurantaa, sekä menetelmiä asiattomien ulkopuolisten tahojen pääsyn estämiseksi järjestelmiin.

Yhteenveto tehdystä kyselystä osoittaa, että kaksi kolmesta vastaajasta on sijoittanut toiminnan turvallisuuden oikeanpuoleiseen alalohkoon ja kolmas vastaaja vasempaan alalohkoon. Vastausten keskiarvona tämän osa-alueen sijainti osuu oikeanpuoleiseen alalohkoon, mikä merkitsee että kyseisen osa-alueen aiheuttamat kustannukset ovat suuret, mutta tietoturvatapahtuman todennäköisyys on pieni, näin ollen kyseistä osa-aluetta ei pidetä merkittävänä riskinä SystemIntelligence Oy:lle.

Perusteluna vastausten sijoittumiselle on pääasiassa se, että ohjelmistojen käyttöönotto, dokumentointi, käyttäjätunnusten ja käyttövaltuuksien hallinnointi ovat osa SystemIntelligence Oy:n omaa ydinosaamista. Yrityksen toiminta perustuu ohjelmistotuotteen kaupallistamiseen ja kyseisen

ohjelmiston uusien piirteiden tuomiseen eri asiakkaille ja seuraaviin versioihin. Dokumentointi ja versioiden hallinta on luonnollinen osa normaalia päivittäistä liiketoimintaa. Myös SystemIntelligence Oy:n sisällä on omalla ohjelmistotuotteella vankka jalansija ja tätä kautta kyseinen riski on alhainen myös omassa toiminnassa.

Eräs vastaajista tosin piti riskiä suurempana kuin muut. Kyseessä on Office Manager, joka omassa toiminnassaan törmää muita vastaajia useammin myös muihin sovelluksiin esim. varusohjelmien uusiin versioihin, joiden käyttöönotto yrityksessä tapahtuu ilman erillistä ohjelmisto- tai integraatiotestausta. Luottavainen suhtautuminen tähän osa-alueeseen johtuu siis pääosin oman tuotteen käytöstä.

Käyttäjätunnukset ovat myöskin oleellinen osa omaa tuotetta ja yrityksessä on ymmärretty niiden merkitys käyttövaltuuksien kannalta. Niiden hallinnointi ei aiheuta ongelmia SystemIntelligence Oy:ssä.

4.2.3. Varkauksilta suojautuminen

Varkauksilta suojautuminen pitää Finnen mallin mukaan sisällään mm. hälyttimien käytön sekä muut fyysiset pääsykontrollit.

Saatujen vastausten perusteella varkauksilta suojautuminen sijoittuu nelikentässä melko alhaisten kustannusten luokkaan ja todennäköisyydeltään keskivälille. Tämän kohdan vastauksista voidaan tehdä päätelmä, että vastaus riippuu kyseisen henkilön tehtävän luonteesta. Teknisemmät henkilöt ovat fokusoituneet vastauksissaan SystemIntelligence Oy:n oman kaupallisen tuotteen turvallisuuteen, joka onkin hyvin hallussa. Palvelimet sijaitsevat ulkopuolisen palveluntarjoajan tiloissa. Myös yrityksen omassa konttorissa

fyysinen suojautuminen on hyvällä mallilla: ala-aulassa on vastaanotto, josta ulkopuoliset pääsevät kerroksiin vain ohjatusti. Lisäksi SystemIntelligence Oy:n tiloihin tullaan kahden kulunvalvonnan piiriin kuuluvan oven kautta.

Hallinnollisesta näkökulmasta katsottuna korostuvat puolestaan omassa käytössä olevat laitteet, jotka eivät ole turvamerkittyjä eivätkä lukittuja vaikka työasemat ovat liikkuvien työntekijöiden mukana oman toimiston ulkopuolella päivittäin. Messukoneet lukitaan messujen ajaksi kiinni kalusteisiin.

4.2.4. Tulipalolta suojautuminen

Tulipalolta suojautuminen tarkoittaa palo- ja savuilmaisimia, sprinklereitä sekä paloturvallisia kassa- / datakaappeja.

Yleisin syy tietokoneiden fyysiselle vahingoittumiselle on tulipalo. Vaikka itse laite ei olisi alttiina tulelle, aiheuttavat savu, noki, kuumuus ja vesi tuhoja laitetiloissa. Tulipaloriskin pienentämiseksi olisi laitetiloissa vältettävä paloherkkiä, pölyäviä ja sähköä kehittäviä materiaaleja.

Vahinkojen minimoimiseksi tulisi jokaiseen laitetilaan asentaa tarvittavat hälytinjärjestelmät sekä savu-, lämpö- ja kosteusilmaisimet. Myös alkusammutusvälineiden saatavuudella ja niiden käyttöön kouluttautumisella voidaan vaikuttaa jo syntyneen vahingon suuruuteen.

Kyselyyn saatujen vastausten perusteella vastaajat ovat tämän osa-alueen suhteen varsin yksimielisiä. Tulipalon todennäköisyyttä pidetään pienenä, mutta mikäli sellainen tapahtuisi, olisivat kustannukset suuret. Vastauksissa ei selvästikään ole huomioitu sitä, että yrityksen vakuutukset kattavat tulipalotapauksessa koituvat aineelliset vahingot, eli riski on siirretty

vakuutusyhtiölle. Näin ollen riski ei SystemIntelligence Oy:n kannalta ole merkittävä.

Omien toimistotilojen suhteen paloturvallisuus on kohtuullisen hyvä, sillä hälyttimet ja sprinklerit ovat asennettuna vuokranantajan toimesta kaikkiin toimistotiloihin. Palonkestäviä arkistokaappeja ei tiedettävästi ole (tai ainakaan ei käytetä). Varmuuskopioiden säilyttäminen muualla kuin palvelintilassa on kunnossa ainakin osittain. Toiminnan kannalta kriittinen seikka on luonnollisesti oman ohjelmiston lähdekoodi, joka on suojattuna vahingoilta Helsingin kauppakamarin Escrow servicessä.

4.2.5. Vesivahingoilta suojautuminen

Vesivahingolta suojautuminen pitää sisältää rakennusmateriaalien ja rakenteiden vedenkestävyyden, vesitunnistimien käytön sekä tulvalta suojautumisen.

Saatujen vastausten perusteella tämä osa-alue on varsin huonosti hoidettu, mutta toisaalta vesivahingon riskiä pidetään vain keskinkertaisena. Ottaen huomioon, että SystemIntelligence Oy toimii vuokratiloissa ja kolmannessa kerroksessa, ei rakenteiden osalta ole paljoakaan tehtävissä. Toisaalta yrityksen omissa tiloissa ei sijaitse kriittisiä palvelimia, joten mahdollinen vesivahinko yrityksen omissa tiloissa ei vaikuta suurelta riskiltä. Palveluntarjoajan tiloissa vesivahinko luonnollisesti saattaa vahingoittaa SystemIntelligence Oy:n tiedostoja. Vastauksissa on selkeästi luotettu siihen, että vesivahingolta suojautuminen on osa palvelinhotellin ydinosaamista ja sitä kautta asioiden pitäisi olla kunnossa.

4.2.6. Virranjakelun varmistaminen

Sähkökatkokset tai suuret vaihtelut virransyötössä saattavat aiheuttaa sen, että kaikki tallentamattomat tiedot menetetään. Yrityksen tulisikin kartoittaa tarpeensa virransyötön varmistamiseksi. Mikäli yritykselle riittää katkeamaton virransyöttö lyhyeksi ajaksi, jolloin tallentamattomat tiedot ehditään tallentaa ennen virran lopullista katkeamista, on ratkaisu UPS. Mikäli taas yrityksen toiminta on tietojärjestelmien suhteen kriittistä, eikä toiminta kestä virransyötön katkoksia lainkaan, on yrityksen syytä hankkia käyttöönsä varavoimaa sähkökatkosten ajalle.

Annettujen vastausten perusteella virranjakelun keskeytymistä ei pidetä suurena riskinä SystemIntelligence Oy:n toiminnalle (sijoittuu keskimäärin vasempaan alalohkoon). Yrityksen toimitiloissa on työasemille käytössä UPS, jonka riittävyys on noin puoli tuntia. Yrityksen kannalta kriittistä on jälleen oman tuotteen palvelimien tilanne. Oletuksena on, että palvelinhotellin palveluntarjoajalla on asianmukainen varavoima käytössään pidempiaikaisten sähkökatkosten varalle. Yrityksen toiminnan kannalta häiritsevä virranjakelun keskeytys on noin puoli tuntia tai enemmän.

4.2.7. Ulkoiset ja sisäiset uhkatekijät

Tietojärjestelmä voi vahingoittua useiden eri uhkatekijöiden vaikutuksesta: tiedon varastaminen, tiedon manipulointi, tietokoneajan varastaminen, ohjelma- tai laitevarkaus, lakko, sabotaasi, kapina, virukset, tietokonerikokset (Turban ym. 1999, 663). Finnen mallissa ulkoisilla ja sisäisillä uhkatekijöillä tarkoitetaan kuitenkin lähinnä sabotaasia ja vakoilua.

Nelikenttätutkimuksen tulokset kertovat varsin yksimielisestä vastaajajoukosta. Yleisesti sabotaasin ja vakoilun todennäköisyyttä pidettiin pienenä, mutta vahinkoja suurena, mikäli SystemIntelligence Oy joutuisi näiden kohteeksi. Vakoilun uhkaa ei kuitenkaan pidetty täysin epätodennäköisenä, toisin kuin useissa yrityksissä Suomessa vielä pidetään.

4.2.8. Tietoliikenne

Nykyisin käytössä olevat ja yhä yleistyvät hajautetut järjestelmät aiheuttavat tarpeen siirtää tietoa paikasta toiseen. Myös yritysten rakenteen muuttuminen yhä useammin useista eri toimipisteistä muodostuvaksi kokonaisuudeksi aiheuttaa informaation siirrolle uusia tarpeita. Lisäksi työnkuva on useilla aloilla muuttunut kiihtyvän työtahdin myötä riippuvaiseksi etätyömahdollisuuksista. Kaikki nämä seikat lisäävät jatkuvasti tiedonsiirron tarvetta ja sen myötä myös tarvetta suojata liikuteltavaa tietoa uteliailta ulkopuolisilta tahoilta.

Kyselyvastausten perusteella SystemIntelligence Oy:ssä ei tietoliikenneriskiä koeta todelliseksi. Keskiarvona tämä osa-alue sijoittuu niukasti nelikentän oikeaan alalohkoon.

Suurimman tietoliikenneriskin SystemIntelligence Oy:n toiminnassa muodostaa etäkäytössä yleistyneet langattomat lähiverkot, joita ei ole suojattu.

4.2.9. Toimintasuunnitelmat

Suunnittelemalla etukäteen miten toimitaan vahinkotilanteessa, voidaan aiheutuvia vahinkoja pienentää huomattavasti. Tehtyjen toimintasuunnitelmien tulee aina olla ylimmän johdon hyväksymiä.

Finnen mallin mukaan toimintasuunnitelma sisältää suunnitelmat itse vahinkotapahtuman varalle, sekä toipumissuunnitelman vahingon jälkeiselle toiminnalle.Toipumissuunnitelman tavoitteena on toiminnan palauttaminen normaaliksi.

SystemIntelligence Oy:n kyselyvastauksissa tämä tietoturvan osa-alue oli eri vastaajien toimesta arvioitu hyvin eri tavoilla. Itse asiassa kaikkien kolmen vastaajan vastaukset osuvat nelikentän eri lohkoihin, ainoastaan pientä todennäköisyyttä ja pieniä kustannuksia vastaava lohko on jäänyt tyhjäksi. Vastausten perusteella on analyysin tässä vaiheessa tehty johtopäätös, että tämä tietoturvallisuuden osa-alue on kohdeyrityksessä ongelmallinen, sillä näiden hajanaisten vastausten yhteinen tekijä on joka tapauksessa korkea riski jomman kumman tai molempien tekijöiden osalta.

Tarkentavia vastauksia tarkasteltaessa selviää SystemIntelligence Oy:n osalta, että yrityksessä ei ole olemassa minkäänlaisia toimintaohjeita tietoturvavahingon varalta, varajärjestelmää ei ole testattu (mikäli sellainen on), eikä toipumissuunnitelmaa myöskään ole olemassa.

4.2.10.Henkilöstöturvallisuus

Tutkimusten mukaan suurin tietojärjestelmiin kohdistuva riski on henkilöriski. Tietoturvan kannalta yritykselle vahingollisimpia ovat tietämättömät

työntekijät, joiden kohdalla inhimillisen virheen todennäköisyys on suuri. Toisen riskiryhmän muodostavat yrityksen entiset työntekijät tai henkilöt, joilla muusta syystä on aihetta tarkoituksellisesti yrittää vahingoittaa yritystä.

Finnen mallin mukaan henkilöstöturvallisuus sisältää ainakin seuraavia osa-alueita:

- rekrytointi: uuden henkilön taustojen selvittäminen
- henkilöstön kontrollit: kulunvalvonta
- pääsy tietoon ja tiedostoihin
- inhimilliset virheet
- alihankkijan työntekijät ja vieraat yrityksen tiloissa
- työpaikkavarkaudet
- tietoturvapäällikkö
- tietoturvakoulutuksen järjestäminen

Nelikenttäkyselyn tulosten perusteella voidaan SystemIntelligence Oy:n osalta todeta, että vastauksissa on merkittävää hajontaa. Kaksi kolmesta vastaajasta kuitenkin sijoittaa henkilöstöturvallisuuden vähintään toisen osatekijän suhteen luokkaan "suuri", joten keskiarvona henkilöstöturvallisuusriski on todennäköinen, mutta vahingon aiheuttama kustannus ei olisi kovin merkittävä. Eräs vastaaja on kuitenkin sijoittanut henkilöstöturvallisuuden omassa nelikentässään kohtaan, joka osoittaa erittäin suuria kustannuksia, mutta todennäköisyys tämänkaltaiseen vahinkoon olisi pieni. Tässäkin tapauksessa kuitenkin toisen riskitekijän ollessa suuri, on tuloksena myös suhteellisen merkittävä riski.

Asioita, jotka nousevat esille annetuista kommenteista, ovat mm. tietoturvapäällikön puuttuminen yrityksestä, joka kuitenkin on IT –alan yritys. Myöskään minkäänlaista tietoturvakoulutusta ei yrityksessä ole järjestetty.

Fyysinen henkilöstöturvallisuus SystemIntelligence Oy:ssä on hoidettu hyvin, sillä yrityksen toimitilat sijaitsevat erään pörssiyhtiön tiloissa, mikä merkitsee tarkkaa kontrollia myös SystemIntelligence Oy:n vierailijoille.

4.2.11.Asenteet tietoturvaa kohtaan

Kirjallisessa muodossa oleva tietoturvapolicy ja olemassa oleva (tiedostettu) tietoturvakulttuuri ovat Finnen mukaan tärkeimmät tekijät arvioitaessa yritysten asenteita tietoturvaa kohtaan.

SystemIntelligence Oy:ssä ei annettujen vastausten perusteella ole olemassa kirjallista tietoturvapolicyä. Myöskään varsinaista tietoista tietoturvakulttuuria ei ole olemassa, on tapoja toimia. Toimintatavat ovat enemmän asiakasrajapinnasta tulevia vaatimuksia kuin yrityksen itsensä kannalta luotuja sääntöjä. SystemIntelligence Oy:ssä ei myöskään ole määritelty sanktioituja tietoturvarikkomuksia.

Nelikentän tarkastelu osoittaa, että jälleen vastaukset ovat kovin hajallaan, mutta kaikkien vastausten keskiarvoa arvioitaessa se saa arvon, joka sijoittuu kustannuksiltaan suuren vahingon puolelle ja todennäköisyys tämänkaltaisen tietoturvatapahtuman esiintymiselle on keskinkertainen. Näin ollen kokonaisriski on melko suuri.

4.2.12.Muut turvallisuusasiat

Muihin turvallisuusasioihin on tässä yhteydessä sijoitettu tietoturvariskit, jotka eivät kuulu edellä mainittuihin ryhmiin. Tähän osa-alueeseen kuuluvia asioita ovat mm.

- paperitulosteiden käsittely

- dokumenttien säilytys
- lämpötila, pöly, savu, ym. Ilman epäpuhtaudet
- olan yli kurkkiminen (shoulder surfing)
- kiinteistöturvallisuus
- postinkäsittelyn turvallisuus / luottamuksellisuus

SystemIntelligence Oy:ssä ei ole käytössä tulosteiden tietoturvaluokituksia, luottamuksellinen tieto tuhotaan silppurissa. Dokumenttien säilytys ei ole kovinkaan relevantti asia muiden kuin hallinnollisten henkilöiden osalta, muilla ei juuri ole dokumentteja kuin sähköisessä muodossa.

Ympäristössä ja ilmassa esiintyviä mahdollisia epäpuhtauksia yrityksessä ei seurata millään tavoin, mutta siivoojille on erillinen ohjeistus pölyn poistamiseksi, lisäksi palvelimia säilytetään viileämmissä tiloissa.

Kiinteistöturvallisuus on hoidettu hyvin, kuten on käynyt ilmi jo aikaisemmissa kohdissa käsiteltäessä kiinteistöön liittyviä asioita. Saapuvien postien käsittely hoidetaan ensisijaisesti lähetyksessä mainitulle vastaanottajalle avaamattomana, muut lähetykset avataan toimitusjohtajan tai Office Managerin toimesta.

Tässä kyselyssä ei esiintynyt merkittäviä puutteita tai ongelmia tällä tietoturvallisuuden osa-alueella, joka keskiarvona sijoittuu melko lähelle nelikentän keskikohtaa.

4.3. Rikastaminen

Ensimmäisen vaiheen tulosten perusteella seuraavaan vaiheeseen valitaan edellä käsitellyistä tietoturvallisuuden osa-alueista ne, joiden kohdalla SystemIntelligence Oy:ssä näyttäisi olevan suurimmat tietoturvariskit.

Valintaprosessi analyysin toiseen vaiheeseen käyttäen aikaisemmin kuvattua "rikastamista" tarkoittaa, että vähintään ne Finnen mallin mukaiset osa-alueet, jotka saavat molempien riskitekijöiden suhteen kyselytutkimuksessa arvon "suuri", tulevat valituksi tarkempaan käsittelyyn.

Edellä saatuja vastauksia sijoitettaessa yhteenvetotaulukkoon (liite 4), voidaan havaita, että ainoastaan yksi kahdestatoista osa-alueesta sijoittuu sekä riskin suuruuden, että todennäköisyyden suhteen lohkoon "suuri". Koska vain yhden osa-alueen ottaminen jatkotarkasteluun tuntuu epätodelliselta, on tässä valittu joitain osa-alueita jatkoon myös kummastakin niistä lohkoista, joissa jompi kumpi riskitekijä saa arvon "suuri".

Analysoimalla melko korkean riskin omaavia osa-alueita (kustannukset tai todennäköisyys suuri) ja peilaamalla niitä edellä esitetyn kyselytutkimuksen vapaisiin kommentteihin, voidaan joukosta poimia muutama sellainen tietoturvallisuuden osa-alue, jotka SystemIntelligence Oy:ssä ovat selvästi tarkemman tutkimisen arvoisia.

Toisen vaiheen analyysiin, jossa käydään tarkemmin kutakin osa-aluetta läpi Finnen mallin mukaisesti, on tässä työssä valittu alla olevat tietoturvaketjun "lenkit". Suluissa on kyseisen osa-alueen saamat arvot nelikenttäanalyysissä (kustannukset, todennäköisyys).

- Toimintasuunnitelmat (suuri, suuri)
- Tietokoneturvallisuus (pieni, suuri)
- Henkilöstöturvallisuus (pieni, suuri)
- Ulkoiset ja sisäiset uhkatekijät (suuri, pieni)
- Asenteet tietoturvaa kohtaan (suuri, pieni)

4.4. Analyysin toinen vaihe

Analyysin toisessa vaiheessa keskitytään ensimmäisessä vaiheessa rikastamisen jälkeen jäljelle jääneisiin tietoturvaketjun lenkkeihin. Toisen vaiheen analyysi käydään läpi Finnen mallin mukaista osa-aluejakoa noudattaen.

4.4.1. Toimintasuunnitelmat

Finnen mallin toimintasuunnitelmat sisältää kaksi osa-aluetta: varautumissuunnitelman (Emergency) ja toipumissuunnitelman (Recovery). Varautumissuunnitelman tarkoituksena on tietoturvatapahtuman sattuessa pienentää vahinkojen suuruutta ja toipumissuunnitelman tarkoitus on palauttaa yrityksen toiminnot normaaleiksi (Finne 1998, 78). Toimintasuunnitelmia tulisi testata säännöllisesti ja raportoida tulokset yrityksen johdolle (Finne 1998, 309). Suunnitelmat tulisi tehdä kirjallisesti kaikista yleisimmistä käytössä olevista järjestelmistä ja sovelluksista. Suunnitelmat tulisi pitää ajan tasalla ja testata säännöllisesti (Daler ym. 1989, 78).

Tutkittaessa kohdeyrityksen toimintasuunnitelmia, on ensimmäinen merkittävä seikka se, että suunnitelmia ei ole olemassa. SytemIntelligence Oy:ssä ei ole olemassa minkäänlaista kirjallista dokumenttia, jossa olisi kerrottu edes yleisellä tasolla mitä tulisi tehdä, mikäli yrityksessä sattuisi jokin

tietoturvatapahtuma. Todennäköistä kuitenkin on, että yrityksen henkilöstöllä on jonkinlainen käsitys tarvittavista toimenpiteistä ainakin yleisimpien tapahtumien varalta.

Koska SystemIntelligence Oy on hyvin tietointensiivinen yritys, tulisi yrityksessä olla selkeästi analysoituna mitkä toiminnot ovat kriittisiä ja mitkä vähemmän kriittisiä. Kriittisyysluokituksen perusteella yrityksessä tulisi voida tehdä arvio, kuinka kauan organisaatio tulee toimeen ilman tietojärjestelmiä. Tästä arviosta käytetään myös nimitystä Maximum Time to Belly Up (MTBU) (Finne 1998, 121). Organisaatiot, jotka ovat vähemmän riippuvaisia tietojärjestelmistä, tulevat toimeen pienemmillä investoinneilla toimintasuunnitelmiin kuin yritykset, jotka ovat hyvin riippuvaisia tietojärjestelmistä, kuten SystemIntelligence Oy.

Toipumissuunnitelman tulisi sisältää tietoa mm. laite- ja ohelmistotoimittajien kanssa tehdyistä sopimuksista, joilla on varmistettu laitteiden ja ohjelmistojen nopea saatavuus mahdollisen katastrofin jälkeen. Edellisen lisäksi nopea toipuminen edellyttää luonnollisesti, että varmuuskopiointi on hoidettu asianmukaisesti ja että laitteet ja ohjelmistot ovat hyvin dokumentoituina.

Kohdeyrityksessä ei ole olemassa toipumissuunnitelmien tarkoittamia sopimuksia toimittajien kanssa. Toisaalta voidaan myös todeta, että yrityksen käyttämät laitteet ovat stardardityöasemia, joiden saatavuus ei pitäisi olla ongelma. Ohjelmistojen saatavuus yrityksen omaa sovellusta lukuunottamatta ei myöskään pitäisi olla hankalaa.

Yrityksen oma sovellus on palvelimella, jonka hoito on ulkoistettu. Ainakin yhdessä kyselyn vastauksista tuli esille se, että kohdeyrityksen ei tarvitse olla huolissaan ulkoistetulla palvelimella sijaitsevasta sovelluksestaan, sillä riski

kyseiseen sovellukseen ja palvelimeen liittyen on siirretty palveluntarjoajalle sopimuksen turvin. Kohdeyrityksen tulisi kuitenkin varmistua siitä, että palveluntarjoajalla on asianmukaiset toimintasuunnitelmat olemassa.

Kohdeyrityksen omaan tuotekehitykseen käytettävät laitteet on hallinnoitu yrityksen omin voimin. Myöskään tuotekehityksellä ei ole toimintasuunnitelmia tai varajärjestelmää, jonka toimivuutta voitaisiin testata säännöllisesti.

Toimintasuunnitelmat näyttävät olevan kohdeyrityksessä varsin heikosti hoidettuna. Yrityksen henkilöstön osaaminen on kylläkin tasolla, jolla näitä asioita on varmasti pohdittu pienemmissä ryhmissä. Tietoisuuden puuttuminen on kuitenkin toistaiseksi aiheuttanut sen, että yrityksessä ei ole virallisia ja dokumentoituja suunnitelmia laadittuna.

4.4.2. Tietokoneturvallisuus

Varmuuskopiointi (Back-Up) on eräs tietokoneturvallisuuden kulmakivistä. Jokaisessa yrityksessä tulisi olla aukoton menetelmä kaiken tarpeellisen tiedon varmuuskopiointiin. Usein päivittäinen rutiini koetaan kuitenkin ajan haaskaukseksi – kunnes sitä tarvitaan.

SystemIntelligence Oy:ssä varmuuskopiointi on systemaattisesti hoidettuna siltä osin kun järjestelmät ovat yrityksen omassa hoidossa. Varmistukset otetaan päivittäin yrityksen tuotekehitysympäristöstä tuotekehityshenkilöstön toimesta, mutta muista järjestelmistä varmistuksia ei oteta.

Henkilökohtaisten työasemien varmuuskopiointi ei yrityksessä ole kenenkään vastuulla keskitetysti, vaan jokaisen työntekijän tulisi itse huolehtia oman työasemansa tietojen varmistuksesta säännöllisesti. Varmistusten ottaminen

jää siten puutteelliseksi, koska kunnollista ohjeistusta asiasta ei ole olemassa. Yrityksessä käytetään asiakirjojen ja dokumenttien säilytykseen yrityksen omaa järjestelmää, jonka palvelimen hoito on ulkoistettuna. Ulkoistuksen osalta varmistukset perustuvat siihen, että toimittaja todella ottaa sovitut varmistukset päivittäin, eikä tässä palvelussa ole havaittu puutteita.

Ongelman tietojen ja dokumenttien hallinnassa aiheuttaa se, että yrityksen teknisen henkilöstön mielestä tietoturva-asiat ovat hoidossa. Tämä käsitys perustuu oletukseen, että kaikki tieto on tallennettuna yrityksen omaan järjestelmään, eikä käyttäjien henkilökohtaisille työasemille. Käytännössä yrityksessä on olemassa merkittävä määrä ns. hallinnollista materiaalia, joka ei koskaan päädy yrityksen järjestelmään, vaan asiakirjoja säilytetään nimenomaan työasemien kovalevyillä. Todennäköisesti myös muuta teknisempää dokumentaatiota säilytetään oman järjestelmän lisäksi työasemilla, sillä vaikka oma järjestelmä onkin käytettävissä selaimella mistä käsin hyvänsä, ei pääsyä internetiin kuitenkaan ole saatavilla aina kun tarvetta olisi. Omien työasemien ongelma ei niinkään aina ole tiedon häviäminen, sillä tiedot ovat todennäköisemmin tallennettuna sekä yrityksen järjestelmään, että henkilökohtaisen työaseman kovalevylle. Ongelmana saattaa kuitenkin olla tietojen joutuminen vääriin käsiin esim. kannettavan työaseman kadotessa.

Varmuuskopioiden säilyttäminen yrityksen ulkopuolella (Off-site storage) on tietokoneturvallisuuden kannalta tärkeää. Varmistettua tietoa sisältävät tallennusvälineet tulisi säilyttää paikassa, jossa ne eivät ole uhattuna mikäli yrityksen tiloissa tai laitetiloissa sattuisi esim. tulipalo.

SystemIntelligence Oy:n varmuuskopiot sijaitsevat pääosin palvelinhotellin tarkoitukseen varaamassa paikassa, jonka turvallisuutta ei

SystemIntelligencen toimesta ole varmistettu. Yrityksen itsensä ottamat varmuuskopiot sijaitsevat samassa laitetilassa yrityksen hallinnassa olevien palvelimien kanssa (Software Developer, 17.3.2005). Yrityksen oman tuotteen lähdekoodi sen sijaan on asianmukaisesti varmistettuna ja annettuna ulkopuolisen palveluyrityksen hoitoon tähän tarkoitukseen varta vasten osoitetussa paikassa.

Tietojärjestelmien toimintakuntoon saattaminen nopeasti esim. tulipalon tai tulvan jälkeen on tietointensiiviselle yritykselle ensiarvoisen tärkeää. Nopeata toipumista helpottamaan on mahdollista vuokrata varalle valmis laitetila (cold site), jossa on järjestettynä virranjakelu, puhelinlinjat, korotettu lattia sekä ilmastointi. Vain laitteet puuttuvat, ja usein niidenkin nopea saatavuus on jo etukäteen varmistettu sopimuksin. Vaihtoehtoisesti yritys voi vuokrata valmiin tilan laitteineen, jotka on konfiguroitu asiakkaan tarpeiden mukaan (hot site) (Daler ym. 1989, 117-118).

SystemIntelligence Oy:llä ei ole olemassa olevaa sopimusta valmiista laitetiloista katastrofin varalle. Toisaalta jälleen kerran luotetaan siihen, että palvelinhotelli on omalta osaltaan varmistanut cold/hot site –sopimukset , joiden turvin myös kohdeyrityksen palvelujen saatavuus on turvattuna.

Menetelmät, joilla voidaan rajoittaa pääsyä tietojärjestelmiin, ovat nykyään kehittyneitä verrattuna entisiin salasanakontrolleihin. Nykyaikaisempia menetelmiä pääsyn rajoittamiseksi ovat esim. biometriset tunnisteet ja älykortit. Biometriset tunnisteet, esim. sormenjälki tai iiris, ovat hyvin luotettavia menetelmiä, mutta niiden heikkoutena vielä nykyään on korkea hinta. Kehittyneempiä menetelmiä voidaan myös yhdistää perinteisiin salasanoihin, jolloin luotettavuus kasvaa entisestään.

Kohdeyrityksessä ei ole käytössä muita pääsykontrolleja kuin salasanat ja normaali kiinteistön kulunvalvonta. Kiinteistöön pääsyä on rajoitettu vuokranantajan toimesta, mikä lisää turvallisuutta. SystemIntelligencen tapauksessa tuntuisi riittävältä nykyinen suojaustaso, varsinkin kun yrityksen henkilöstömäärä on niin alhainen, että ulkopuolisten on mahdotonta päästä yrityksen tiloihin huomaamatta. Salasanojen vaihtuvuuteen ja pituuteen tulisi kuitenkin kiinnittää huomiota.

Tietojen tallennusta ulkopuolisille tallennusvälineille voidaan yrityksissä rajoittaa asentamalle yrityksen työasemiin lukot, joilla estetään tietojen luvaton tallentaminen levykkeille. Toinen tapa estää tallentamista on hankkia työasemia, joissa ei ole levyasemaa. Edellä esitetyt menetelmät sopivat kohdeyritystä paremmin suuriin yrityksiin, joissa tietojen tallennusta ja asiattomien henkilöiden pääsyä työasemien läheisyyteen on muuten vaikea valvoa.

Tietojen salaus, eli kryptaus, on edelleenkin suhteellisen vähän käytetty menetelmä, joskin parhaita tapoja suojata arkaluontoista tietoa (Finne 1998, 300). Yleensä tiedostojen salauksella halutaan varmistaa tiedon luottamuksellisuuden säilyminen. Salauksella pyritään varmistamaan, että vaikka joku ulkopuolinen pääsisi urkkimaan tiedonsiirtoa tai saisi tiedoston haltuunsa, esim.vahingossa väärään osoitteeseen lähetetyn sähköpostin tiedostoliitteenä, hän ei pystyisi näkemään tiedoston sisältöä.

SystemIntelligence Oy:ssä tietoja salataan ainoastaan tiedonsiirron ajaksi. Yrityksen työntekijöistä suurin osa käyttää työssään kannettavia työasemia, minkä vuoksi olisikin tarpeen ajatella tietojen salaamista myös työasemien kovalevyllä. SystemIntelligencessä on myös tällä hetkellä varsin runsas joukko henkilöitä, joilla on yrityksen omaan järjestelmään administrator –

oikeudet. Tämä oma tuote on paikka, johon on tallennettuna myös sellaisia, esim. työsuhteisiin liittyviä tietoja, joiden paljastuminen edes järjestelmän pääkäyttäjille ei ole tarpeellista, varsinkaan kun pääkäyttäjiä on useita. Tietojen salaaminen olisikin menetelmä, jolla myös pääkäyttäjien pääsyä arkaluontoiseen tietoon voitaisiin rajoittaa.

Tiedostoihin pääsyn turvallisuus on luottamuksellisuutta. Käyttövaltuuksien ja asianmukaisten salasanojen avulla yrityksen tulee varmistaa, että vain valtuutetut henkilöt pääsevät käsiksi yrityksen tiedostoihin ja lähiverkkoon. Yleisin vaihtoehto käyttäjän tunnistamiseksi on pelkkä salasana ja käyttäjätunnus eri muunnelmineen. Se on käytettävyydeltään ja ylläpidettävyydeltään helpoin valinta, vaikka käyttäjän määrittämät ja muistamat salasanat ovatkin inhimillisen tekijän vuoksi usein koko järjestelmän heikoin lenkki.

Kiusaus käyttää helppoja ja samoja salasanoja on suuri. Huonojen salasanojen käyttö on useissa yrityksissä merkittävä uhka koko tietojärjestelmän turvallisuudelle. Vaikka salasana pakotetaankin vaihtamaan kuukauden välein ja uusi ei saa olla sama kuin kahdella edellisellä kerralla, ja pituuden on oltava vähintään kahdeksan merkkiä, on huonoja salasanoja liian helppo keksiä. Turvallisuutta voidaan parantaa erillisellä suodatuksella, jolla voidaan estää laittamasta salasanoiksi esimerkiksi perinteisiä automerkkejä tai suosikkijuomia.

Yritysten tulisikin säännöllisesti testata salasanansa murto-ohjelmilla ja ohjeistaa huonon salasanan valinneita työntekijöitä salasanan valinnassa. Hyvänkin salasanan selville saaminen on usein erittäin helppoa. Usein saattaa riittää, että soittaja esiintyy tietojärjestelmän ylläpitäjän nimikkeellä (salasanojen sosiaalinen selvittäminen).

Koska turvallisten salasanojen keksiminen on lähes mahdoton tehtävä, tullaankin tulevaisuudessa yhä enemmän keskittymään muiden kuin aakkosnumeeristen tai erikoismerkkejä sisältävien salasanojen käyttöön. Perinteisiä salasanoja turvallisempia vaihtoehtoja ovat tässä työssä jo aiemmin käsitellyt erilaiset toimikortit, tai käyttäjän biometrinen tunnistus (sormenjälki, ääninäyte, iiris) tai näiden yhdistelmät.

Salasanojen turvallisuuteen ei kohdeyrityksessä ole kiinnitetty erityistä huomiota, eikä asiasta ole olemassa yleisiä ohjeita. Käytössä olevat järjestelmät vaativat sisällöltään ja pituudeltaan erilaisia salasanoja, joten vain yhden salasanan käyttäminen ei ole mahdollista. Käytössä olevat järjestelmät eivät tosin pakota vaihtamaan salasanoja, mutta niiden lukuisuus saattaa aiheuttaa muistamisongelmia.

Tietokonevirus on ohjelmakoodi, joka on suunniteltu täyttämään kaksi tavoitetta: (1) monistaa itsensä tietojärjestelmästä toiseen, (2) päästä käsiksi tietojärjestelmiin siten, että sen on mahdollista muuttaa tai tuhota ohjelmia tai tietoja häiritsemällä käyttöjärjestelmän normaaleja prosesseja (PriceWaterhouse 1990, 1).

Täydellistä suojaa tietokoneviruksilta on tänä päivänä käytännössä mahdotonta saavuttaa, sillä uusien virusten määrä lisääntyy vuosittain eksponentiaalisesti. Yhdistämällä yrityksen management policyn asianmukaisten ja ajantasaisten virustorjuntaohjelmistojen kanssa voidaan virusten aiheuttamaa riskiä pienentää hyväksyttävälle tasolle. Heikkoutena on se, että nämä ohjelmistot toimivat usein vain jo tunnettuja viruksia vastaan (PriceWaterhouse 1990, 34).

SystemIntelligence Oy:ssä käytetään yleisesti saatavilla olevia viruksentorjuntaohjelmistoja toimistosovelluksissa. Yrityksen tuotekehityksessä ja yrityksen omassa järjestelmässä sen sijaan ei viruksentorjuntaa ole käytössä (Software Engineer 15.3.2005). Viruksen siirtyminen yrityksen järjestelmään sinne talletetun dokumentin myötä on kuitenkin mahdollista, joten jonkin asteinen torjunta myös tältä osin olisi suotavaa.

Tulostimet ja fax –laitteet saattavat olla merkittävä tietoturvariski yrityksessä. Verkkotulostimelle tulostettu luokiteltua informaatiota sisältävä tuloste saattaa olla useiden ohikulkijoiden silmäiltävänä ennen kuin sen tulostanut henkilö saapuu noutamaan sen.

SystemIntelligence Oy:ssä tämänkaltainen tilanne on ollut mahdollinen, mutta lähitulevaisuudessa riski on ainakin pienennettävissä, sillä yritykseen on tilattu uusi monitoimilaite. Uuden laitteen avulla tulosteet voidaan ohjata "postilaatikkoon", jonka omistaja purkaa tulosteen henkilökohtaisen koodin avulla vasta saavuttuaan itse laitteen viereen. Näin pienennetään merkittävästi tulosteiden riskiä joutua vääriin käsiin. Faxien osalta tilanne säilyy ennallaan, tosin erillisen "hallinnollisen" faxin käyttöönottoa on harkittu.

Levykkeiden turvallisuus on Finnen mallissa merkittävä tietoturvariski. Finne tarkoittaa erityisesti levykkeiden liikuttamista esim. postin välityksellä paikasta toiseen, jolloin ne saattavat joutua kadoksiin kuljetuksen aikana. Tämä osa-alue on menettänyt merkityksensä tiedonsiirtonopeuksien kasvaessa ja sähköpostin yleistyessä. Yhä vähemmän tietoa lähetetään levykkeellä paikasta toiseen.

Tietokoneajan ostaminen ja ulkoistaminen ovat kasvattaneet yritysten tietoturvariskiä. Ulkoistuskumppanien luotettavuus on ensiarvoisen tärkeää, kun yritys luovuttaa toiminnalleen kriittisen osan toisen yrityksen vastuulle. SystemIntelligence on ulkoistanut omille asiakkailleen tarjoamansa palvelun hoitamisen toiselle yritykselle. Kuten aiemmin tässä työssä on käynyt ilmi, ei SystemIntelligence ole systemaattisesti valvonut kumppaninsa luotettavuutta, mutta toisaalta kyseessä on eräs Suomen suurimmista yhtiöistä, joten riski on pienempi, kuin jos palvelu olisi ulkoistettu jollekin pienehkölle yritykselle.

Tietokonelokien seuranta on eräs tapa havainnoida esimerkiksi yrityksen verkkoon suuntautuneita tunkeutumisyrityksiä. Yksinkertaisimmillaan tunkeutumisen havainnointiin riittää verkkolaitteiden lokien seuranta, sillä asiantunteva henkilö osaa lukea jo niistä mahdollisia tunnustelutrendejä. Verkon tapahtumien seuranta on jatkuva prosessi, se mikä toimi kuukausi sitten, ei välttämättä riitä tänään. Kohdeyrityksessä ei kirjautumisyrityksiä seurata säännöllisesti, mutta satunnaisesti tärkeimmistä paikoista, esim. palvelimilta, joilla on lähdekoodi (Software Engineer 15.3.2005).

Työasemia voidaan lukita esimerkiksi toimistokalusteisiin varkauksien estämiseksi. Kuten on todettu jo useasti tässä työssä, SystemIntelligencen työntekijät käyttävät suurimmaksi osaksi kannettavia työasemia, joiden lukitseminen paikalleen ei tule kyseeseen. Lukitsemisen sijasta yrityksessä on kuitenkin huolehdittu työasemien merkitsemisestä tarroin. Lisäksi laiterekisteri on ajantasalla. Näistä varotoimenpiteistä huolimatta työasemien turvallisuus on todellinen riski SystemIntelligencessä.

4.4.3. Henkilöstöturvallisuus

Tutkimusten mukaan suurin tietojärjestelmiin kohdistuva riski on henkilöriski. Tietoturvan kannalta yritykselle vahingollisimpia ovat tietämättömät työntekijät, joiden kohdalla inhimillisen virheen todennäköisyys on suuri. Toisen riskiryhmän muodostavat yrityksen entiset työntekijät tai henkilöt, joilla muusta syystä on aihetta tarkoituksellisesti yrittää vahingoittaa tiettyä yritystä.

Uuden työntekijän rekrytointi on tärkeä päätös, jonka tueksi yrityksen tulisi aina selvittää palkattavan henkilön taustoja esim. haastattelemalla henkilön aikaisempia työkavereita tai esimiehiä. Mitä tärkeämpään tehtävään palkattava henkilö on tulossa, sitä tärkeämmäksi nousee tietoturva-asioiden selvittäminen. Monissa yrityksissä nykyään pyydetään jo työsopimuksen allekirjoitusvaiheessa työntekijältä suostumus mm. rikosrekisteritietojen selvittämiseen Keskusrikospoliisista.

SystemIntelligencessä ei ole käytössä menetelmää, jossa selvitettäisiin palkattavien henkilöiden taustaa. Syynä tähän saattaa olla se, että ongelmia ei ole esiintynyt henkilöstön luotettavuuden suhteen, lisäksi osa tulokkaista on jo aiemmalta ajalta tuttuja joillekin työntekijöille. Nykytilanteessa siis kohdeyrityksessä luotetaan henkilöstön rehellisyyteen, mutta tulevaisuudesa saattaa olla tarpeen ryhtyä kiinnittämään huomiota myös uusrekrytointeihin. SystemIntelligencessä raja oman henkilöstön ja ulkopuolelta ostettujen palveluiden välillä on melkoisen ohut. Alihankkijoiden kanssa on kuitenkin allekirjoitettu salassapitosopimukset sanktioineen.

Henkilöstön valvonta on eräs tapa suojautua henkilöriskeiltä. Joissain yrityksissä on luotu valvontajärjestelmä, jonka turvin työntekijät voivat anonyymisti raportoida työtovereidensa mahdollisista tietoturvarikkomuksista.

Tämänkaltaiset menetelmät ovat kuitenkin omiaan tuhoamaan työyhteisön viihtyvyyttä. Enemmänkin yrityksissä tulisi kiinnittää huomiota työntekijöiden koulutukseen erityisesti sen suhteen, mitä yrityksestä saa kertoa ulkopuolisille. Ei ole harvinaista, että messuilla ja näyttelyissä vierailee henkilöitä, joiden tarkoituksena on urkkia tietoja yrityksestä haastattelemalla messuilla olevaa henkilöstöä. Kohdeyrityksessä ei ole olemassa menetelmiä henkilöstön toimien valvomiseksi, myöskään yleisesti ei ole olemassa sääntöjä siitä, mitä ulkopuolisille saa kertoa yrityksestä. Sen sijaan SystemIntelligencessä on koulutettu henkilöstöä niiden asiakkaiden suhteen, joista yrityksen henkilöstön ei ole lupa puhua ulkopuolisille. Oma turvallisuus siis ei ole koulutuksen tavoitteena, vaan luottamuksen säilyttäminen asiakkaisiin päin.

Henkilösturvallisuutta voidaan lisätä jakamalla arkaluontoista tietoa vain niille henkilöille, jotka tarvitsevat sitä työssään (need to know –periaate). Kaikki tieto ja pääsy niihin tulisi luokitella seuraavasti (Hannula & Siilasmaa 1991):

a. Salainen tieto, jonkä joutuminen vääriin käsiin saattaa vahingoittaa yritystä vakavasti, esim. strategiat ja tuotekehitys
b. Luottamuksellinen tieto, joka sisältää arkaluontoista informaatiota yrityksestä, esim. budjetit
c. Sisäinen informaatio, jonka joutuminen ulkopuolisten käsiin ei vahingoita yritystä esim. henkilökuntalehti, sisäinen puhelinluettelo
d. Julkinen informaatio, joka yrityksestä halutaan kertoa ulkopuolisille, esim. vuosikertomukset

Käytettävien tietojärjestelmien käyttöoikeudet tulisi luokitella edellä olevaa jakoa noudattaen työtehtävittäin. SystemIntelligencessä ei ole estetty henkilöstön pääsyä erilaisiin tietoihin. Kuten tässä työssä on jo aiemmin

todettu, on yrityksessä useita henkilöitä varustettu ns. administrator – oikeuksin, mikä vähentää oleellisesti tietoturvallisuutta.

Suurin osa valvonta- ja turvaongelmista aiheutuu inhimillisen virheen seurauksena (Turban ym. 1999, 663). Inhimillisellä virheellä tarkoitetaan työntekijän, alihankkijan, toimittajan tms. tekemää virhettä, jonka seurauksena tietoturva vaarantuu tahattomasti. SystemIntelligencessä on virheen mahdollisuutta pyritty vähentämään mm. siten, että yrityksen omassa käytössä on oman tuotteen kehitysympäristö. Näin koko henkilökunta osallistuu päivittäisessä työssään järjestelmän testaukseen. Tämä testaus ei luonnollisestikaan riitä varmistamaan ettei toimitusprojekteissa esiinny virheitä.

Muita Finnen esittämiä henkilöstöturvallisuuden osa-alueita ovat:
-"luvaton työskentely", joka tarkoittaa yrityksen ulkopuolisten tehtävien hoitoa työnantajan ajalla ja laitteilla. Tällaista ei ole erikseen kielletty kohdeyrityksessä, mutta sellaisesta ei myöskään ole havaittu ongelmia. Oletuksena työntekijöillä onkin vapaus käyttää ainakin työnantajan työkäyttöön luovutettua työasemaa muuhunkin kuin työtarkoitukseen työajan ulkopuolella. Työnantajan kanssa kilpailevaa toimintaa ei luonnollisestikaan sallita.
-työvoimapula on omiaan lisäämään tietoturvariskiä. Paineen alaisena ja kiireessä toimittaessa virheiden todennäköisyys kasvaa ja tietoturva-asiat saattavat alkaa tuntua epärelevanteilta ja työntekoa hidastavilta. Tämän tekijän suhteen nykyisellään kohdeyrityksessä on kohonnut riski, sillä tietyissä osissa yritystä on merkittävää pulaa työvoimasta ja rekrytointiprosessi on myöhästynyt ajatellusta aikataulusta, minkä seurauksena nykyisten resurssien jaksaminen on koetuksella. Asiaa yritetään ratkaista mahdollisimman pikaisesti ja yrityksen johto on havainnut ongelman.

-rikollinen toiminta henkilöstön toimesta on myös tietoturvariski. Rikollisuus ei ole ollut ongelmana kohdeyrityksessä, mutta muista syistä on painotettu esim. sitä, että työasemaa ei ole syytä jättää itsekseen taukojen tms. ajaksi siten, että ollaan sisäänkirjautuneena. Työaseman luota poistuttaessa, vaikka vain hetkeksi, tulee aina poistua käyttöjärjestelmästä.

Finnen mukaan jokaisessa yrityksessä tulee olla henkilö, jonka vastuulla on yrityksen tietoturvallisuus. Tämä ei kuitenkaan tarkoita sitä, että kyseisen henkilön tulisi yksinään suoriutua tietoturvan varmistamisesta, vaan sitä että hänelle on osoitettuna resurssit, joiden avulla hän varmistaa tavoitellun tietoturvatason. Tämän tehtävään osoitetun henkilön vastuulla on myös järjestää yrityksessä yleistä tietoturvakoulutusta, sekä varmistaa kirjallisen tietoturvaohjeistuksen olemassaolo. Tietoturvahenkilön tulee myös luoda yritykseen menettelytapa, jolla kerätään tietoa mahdollisista tietoturva-aukoista, ja -rikkeistä, sekä "läheltä piti" –tilanteista. Mikäli näitä tapahtumatietoja ei saada kerättyä yrityksessä, ei niitä vastaan myöskään osata varautua tulevaisuudessa ja näin samankaltainen tapahtuma voi toistua.

SystemIntelligencen organisaatiossa ei varsinaisesti ole resurssoitu tietoturva-asioita kenenkään vastuulle. Tuoteorganisaatiossa on henkilöitä, joiden vastuulla on yrityksen tuotteen turvallisuus, mutta yleishallinnollinen turvallisuus liittyen toimistojärjestelmiin ja muihin yleisiin periaatteisiin on heikosti vastuutettu. Yrityksen talous- ja hallinto-osasto vastaa periaatteessa yleisestä tietoturvasta, mutta tekniset apuresurssit asioiden kuntoon saattamiseksi puuttuvat. Yrityksen sisällä on runsaasti osaamista tietoturva-asioihin liittyen, mutta ongelmaksi muodostuu resursointi. Vastuullisten henkilöiden tulee "lainata" resursseja muilta osastoilta, jotka eivät näe tietoturvaa kriittisenä asiana ja näin priorisoivat asiakastoimitukset sekä

tuotekehityksen tietoturvallisuuden edelle, mikä luonnollisesti on yrityksen liiketoiminnan kannalta järkevää.

4.4.4. Ulkoiset ja sisäiset uhkatekijät

Ulkoiset ja sisäiset uhkatekijät on Finnen mallissa jaettu kolmeen osaan:

- Sabotaasi
- Vakoilu
- Julkinen informaatio

Sabotaasi ja vakoilu ovat molemmat toimintoja, joihin saattavat syyllistyä oman yrityksen työntekijät. Yhä useammin kuitenkin näitä toimintoja suorittaa yrityksen ulkopuolinen taho esim. myyntimies, konsultti, tietokoneen korjaaja tai muu vierailija.

Julkisella informaatiolla tarkoitetaan tässä tietoa, joka on annettu ulkopuoliselle taholle julkaistavaksi tai tutkimuskäyttöön. Tällaisen informaation luovuttaminen yrityksen ulkopuolelle tulisi organisoida yhden henkilön kautta tapahtuvaksi, näin voitaisiin varmistaa, että väärää tai vahingollista tietoa ei päästetä ulos organisaatiosta.

SystemIntelligence Oy:ssa ei sabotaasin mahdollisuuteen juurikaan uskota, sen sijaan vakoilun uhka on todellinen. Lähinnä yrityksen toiminnan kulmakiven, oman tuotteen lähdekoodin, joutuminen vääriin käsiin voi johtaa koko yrityksen toimintaedellytysten lakkaamiseen. Tätä problematiikkaa yrityksessä on viime aikoina käsitelty aktiivisesti. Lähdekoodin suojaaminen pitäisi hoitaa kuntoon viimeistään siinä vaiheessa kun vientitoiminta ulottuu maihin, joissa patentti ei suojaa tuotetta. Kohdeyrityksen kannalta tällainen tilanne saattaa tulla hyvinkin yllättäin, sillä tuotetta saatetaan viedä

eksoottisiin maihin asiakasyritysten laajentaessa toimintaansa esim. Kaukoltään.

Vääränlaisen informaation päätyminen julkisen informaation joukkoon ei kohdeyrityksessä tällä hetkellä ole ongelma. Kaikki julkinen informaatio yrityksestä kulkee pääsääntöisesti toimitusjohtajan kautta, jolloin mahdollisuutta luottamuksellisten tietojen antamiseen erehdyksessä ei ole. Poikkeuksiakin saattaa luonnollisesti olla esim. erilaiset puhelimitse tehtävät tutkimukset saattavat kohdistua sellaisiin henkilöihin, joilla ei ole kykyä arvioida annettavien tietojen luottamuksellisuuden astetta.

4.4.5. Asenteet tietoturvaa kohtaan

Asenteet tietoturvaa kohtaan on Finnen mallissa jaettu kahteen osa-alueeseen:

- Kirjallisessa muodossa oleva tietoturvapolicy
- Tietoturvakulttuuri

Kirjallisessa muodossa oleva tietoturvapolicy on kaiken tietoturvatietoisuuden edellytys yrityksessä. Minimissään sen tulee sisältää tieto siitä, minkä tyyppiset tiedot vaativat suojausta sekä millä toimenpiteillä mitäkin tietoa suojataan. Ohjeistusta tulee myös noudattaa, ylläpitää ja päivittää säännöllisesti.

Kuten on käynyt ilmi jo aiemmin tässä työssä, SystemIntelligence Oy:ssä ei ole käytössä minkäänlaista kirjallista ohjeistusta tietoturvallisuuden suhteen. Ainoastaan asiakkaita koskevaa informaatiota ja sen luottamuksellisuuden tärkeyttä on korostettu henkilöstölle.

Tietoturvakulttuuri ei synny itsestään, vaikka yrityksessä olisikin kirjalliset ohjeistukset tietojen suojaamiseksi. Kulttuurin kehittyminen edellyttää jatkuvaa koulutusta ja tiedottamista, sekä mahdollista palkitsemisjärjestelmää. Tietoturvarikkomuksista voidaan asettaa rangaistuksia ja toisaalta palkita henkilöitä, jotka noudattavat ohjeistusta. Myös tietoturva-aspektin sisällyttäminen tehtäväkuvauksiin on omiaan lisäämään tietoturvakulttuurin syntymistä.

SystemIntelligence Oy:ssä ei ole käytössä sanktioita tietoturvarikkomuksista, eikä myöskään palkintoja ohjeiden noudattamisesta, koska ohjeita ei ole. Yleisesti voitaneen todeta, että kohdeyrityksen henkilöstön moraali tietoturva-asioiden suhteen on melko korkea. Koska rikkomuksia ei ole käytännössä todettu, ei myöskään erityistä kulttuurin luomista ole pidetty niin tärkeänä, että sitä olisi systemaattisesti ryhdytty rakentamaan.

4.5. Analyysin johtopäätökset ja toimenpidesuositukset

Tässä analyysin toisessa vaiheessa on käyty läpi Finnen mallin mukaisesti ne tietoturvaketjun osaset, jotka ensimmäisen vaiheen "rikastamisen" jälkeen jäivät analysoitaviksi.

Ensimmäisenä toisen vaiheen analyysissa käsiteltiin toimintasuunnitelmia. Toimintasuunnitelmat muodostuivat varautumissuunnitelmista ja toipumissuunnitelmista. Analyysin tuloksena selvisi, että kohdeyrityksessä ei ole käytössä minkäänlaisia toimintasuunnitelmia. SystemIntelligencen valittuna IT –strategiana on ollut ulkoistaminen, minkä seurauksena yritys on siirtänyt vastuuta monista tietoturvallisuuteen liittyvistä asioista palveluntarjoajille. Koska varmuuskopiointi ja varajärjestelmien olemassaolon varmistaminen kuuluvat itsestäänselvyyksinä ulkoistamissopimuksiin, ei

SystemIntelligence ole suorittanut auditointia palveluntuottajien todellisesta kyvystä ylläpitää palvelutasoa katastrofin kohdatessa. Riskinä tämänkaltaisissa tilanteissa on mahdollisuus, että palveluntarjoaja ei olekaan hoitanut tietoturva-asioita kuntoon toivotulla tavalla, tai että ne on alimitoitettu.

Yrityksen omassa hoidossa ovat palvelimet, joilla tuotetaan palvelua yrityksen omaan käyttöön. Vaikka palvelu toimiikin samalla ns. testiympäristönä, on sen varassa kuitenkin lähes kaikki yrityksen oma informaatio. Kyseisellä palvelimella ei ole varajärjestelmää, eikä toimintaohjeita mahdollisen katastrofin uhatessa. Varmuuskopiointi hoidetaan lähes päivittäin omin voimin, mutta varmistusnauhat säilytetään palvelintiloissa, joten niiden käytettävyys esim. tulipalon tai vesivahingon sattuessa on vähintäänkin epävarmaa.

Suositeltavia toimenpiteitä toimintasuunnitelmiin liittyen on vähintäänkin niiden olemassaolon varmistaminen. Yrityksessä tulisi olla jonkinlaiset kirjalliset suunnitelmat erilaisten tietoturvauhkien varalle. Lisäksi eri järjestelmillä tulisi olla varajärjestelmät, joiden toimivuutta testataan säännöllisin väliajoin. Kannettavien työasemien saatavuus on melko hyvä, joten niiden osalta ei ole tarpeellista tehdä toimitussopimusta minkään ulkopuolisen laitetoimittajan kanssa. Työasemien osalta riittää, että toipumissuunnitelmaan on kirjattuna luotettava laitetoimittaja, jolta samoja laitteita on hankittu ennenkin. Edellytyksenä on tietysti, että yrityksessä pidättäydytään standardityöasemissa jatkossakin.

Toisena tutkittavana tietoturvaketjun osana oli tietokoneturvallisuus. Varmuuskopiointi on eräs tietokoneturvallisuuden kulmakivi. Kuten on jo aiemmin todettu, ei kohdeyrityksessä juurikaan oteta varmuuskopioita. Säännöllisiä varmistuksia otetaan vain yrityksen omassa hallinnassa olevalta

palvelimelta, jolle on sijoitettu testi- ja kehitysympäristönä toimiva yrityksen itselleen tuottama palvelu. Kuten aiemmin on todettu, varmistusnauhoja säilytetään samassa laitetilassa itse palvelimen kanssa, mikä ei ole tietoturvallisuuden kannalta järkevää. Jokaisella yrityksen työntekijällä on käytössään työasema (yleensä kannettava), joiden kovalevyjen varmuuskopiointi on jätetty kunkin työntekijän omalle vastuulle. Käytännössä varmistuksia ei juurikaan oteta, tosin monet työntekijät tallentavat kaikki dokumentit yrityksen omaan selainpohjaiseen järjestelmään, mikä ei tosin rajaa pois samoja dokumentteja omalta kovalevyltä. Kovalevyllä olevat tiedostot muodostavat tietoturvariskin, mikäli ne joutuvat ulkopuolisten saataville.

SystemIntelligencessä käytetään tiedostojen salausta vain tiedonsiirrossa. Kannettavien työasemien kovalevyillä olevat tiedot koskien esim. asiakasprojekteja ovat salaamattomia ja siten saattavat haavoittaa yrityksen liiketoimintaa joutuessaan vääriin käsiin.

Tärkeimmät suositeltavat toimenpiteet kohdeyritykselle tietokoneturvallisuuteen liittyen ovat

- Varmuuskopioiden säilyttäminen erillään laitetilasta (off-site storage)
- Työasemien kovalevyjen säännöllinen varmuuskopiointi
- Kannettavilla työasemilla olevien tiedostojen salaus
- Virustorjunnan ulottaminen myös omaan järjetelmään

SystemIntelligencessä ei juurikaan ole kiinnitetty huomiota henkilöstöturvallisuuteen. Henkilökunnan kyky arvioida omaa toimintaansa on tähän saakka ollut riittävä tietoturvan tae. Jossain määrin yrityksessä on eletty "lintukotomaista" aikaa, ja jokainen työntekijä on kantanut oman kortensa kekoon. Luottamus työntekijöitä kohtaan on luultavasti ollut omiaan lisäämään

vastuullisuuden tunnetta, mutta siitä huolimatta olisi jatkossa syytä huomioida erityisesti joitain henkilöstöturvallisuuteen liittyviä seikkoja:

- Pääsyn rajoittaminen tietoihin, joita työntekijä ei työssään tarvitse
- Henkilöresurssien mitoittaminen siten, että kiireen ja stressin aiheuttama inhimillisen erehdyksen riski minimoidaan
- Tietoturvavastaavan nimittäminen ja resurssien osoittaminen hänen käyttöönsä
- Tietoturvakoulutuksen lisääminen
- Tietoturvarikkomusten ja läheltä piti –tilanteiden raportointi

Ulkoisten sisäisten uhkatekijöiden merkitys SystemIntelligence Oy:ssä on kasvussa. Kuten aiemmin on todettu, ei sabotaasin todennäköisyys ole kovinkaan todennäköinen, mutta vakoilun uhka sen sijaan on jo nykyään olemassa ja sen todennäköisyys kasvaa yrityksen toiminnan kasvaessa ja saadessa laajempaa merkitystä. Erityisen uhkan, joskin myös mahdollisuuden, SystemIntelligencelle asettaa laajentuminen Kauko-Itään tehtäviin installaatioihin, jolloin yrityksen lähdekoodin kopiointi ja kaupallinen hyödyntäminen on todellinen uhkatekijä. Yrityksestä annettavan julkisen informaation merkitys on myöskin kasvussa. Ulkopuolelle annettavan tiedon merkitys kasvaa yritystoiminnan laajentuessa ja yrityksen saadessa enemmän julkisuutta. Tällöin myös ulkopuolisten tahojen, kuten median kiinnostus yritystä kohtaan saattaa olla haittaavan suurta, mikä asettaa vaatimuksia organisoida ulkoinen viestintä nykyistä virallisemmaksi.

Suositeltavaa ulkoisten ja sisäisten uhkatekijöiden pienentämiseksi olisi ainakin huomion kiinnittäminen myös sabotaasin mahdollisuuteen, jotta tietoisuus olisi herätettynä myös tältä osin. Lisäksi lähdekoodin suojaamisen ratkaiseminen tavalla tai toisella ennen laajentumista Euroopan ulkopuolelle

on edellytys liiketoiminnan jatkumiselle. Kolmantena kehittämiskohteena on viestintäfunktion perustaminen hoitamaan ulkoista viestintää, sekä muistuttamaan henkilökuntaa asioista, joita ei ole sopivaa kommunikoida ulkopuolisille, eikä aina edes yrityksen sisällä. Viestinnän kehittämiseen ei kuitenkaan ole välitöntä tarvetta, ennen kuin ulkopuolinen mielenkiinto kasvaa asettamaan uusia vaatimuksia viestinnälle.

Asennoituminen tietoturvallisuutta kohtaan on SystemIntelligence Oy:ssä hyvin epämuodollista, eli tietoturva-asioita ei ole korostettu jokapäiväisessä toiminnassa. Kirjallisia ohjeita tietoturvallisuuteen vaikuttavien toimintojen suhteen ei ole olemassa ja yrityksessä onkin lähinnä luotettu työntekijöiden oma-aloitteisuuteen ja haluun huolehtia tietoturvasta, sekä myös hyvään onneen. Varsinaista tietoturvakulttuuria ei yrityksessä myöskään ole vaalittu, mutta työntekijöiden korkea koulutustaso ja hyvä tietoturva-asioiden tuntemus ovat vaikuttaneet omalta osaltaan tietoturvakulttuurin syntymiseen.

SystemIntelligence Oy:n tietoturva-asenteiden kohottamiseksi olisi tarpeen laatia kirjallinen tietoturvapolicy, joka tulisi jalkauttaa organisaatioon ja sitä kauttaa levittää yleistä tietoisuutta, tietämystä jo on. Tietoturvapolicyn noudattamista tulisi myös valvoa ja luoda järjestelmä mahdollisten rikkeiden raportoimiseksi. Esiintyvät rikkomukset ja "läheltä piti" tilanteet tulisi käsitellä esimerkiksi yrityksen johtoryhmässä.

Johtopäätöksenä tehdyn analyysin pohjalta voidaan todeta, että SystemIntelligence Oy:n tietoturvan taso ei hallinnollisessa mielessä ole kovin korkea. Yrityksen oman tuotteen turvallisuus on hyvällä tasolla, mikä onkin yrityksen kaupallisen toiminnan perusedellytys, sen sijaan omaan toimintaan vaikuttavien seikkojen on annettu toistaiseksi hoitua omalla painollaan. Syynä tietoturva-asioiden matalaan profiiliin kohdeyrityksessä on ollut yrityksen pieni

koko. Henkilökunta on ollut korkeasti koulutettua, motivoitunutta sekä yrittäjähenkistä. Tietoturva-asioiden painoarvon nostaminen yrityksen liiketoiminnan kasvaessa on kuitenkin hyvin perusteltua edellä käsitellyistä seikoista johtuen.

5. YHTEENVETO

Tämän tutkielman tutkimusongelmana oli pk -yrityksen tietoturvan tason arviointi. Peruslähtökohtana oli selvittää kirjallisuudessa esitettyjen menetelmien toimivuutta kyseisessä arvioinnissa ja löytää sellainen menetelmä, jonka avulla oli mahdollista suorittaa arviointi, sekä löytää mahdollisia kehityskohteita.

Tämä työ muodostuu teoria- ja empiriaosasta. Teoriaosassa määriteltiin aluksi tietoturvaan ja riskeihin liittyvät käsitteet. Käsitteiden jälkeen esiteltiin kirjallisuuden tuntemia menetelmiä pk -yrityksen tietoturvan tason määrittämiseksi. Työssä arvioidut mentelmät ovat arvottaminen, kysymyssarjat, heuristiset menetelmät, sekä Finnen kehittämä Computer-Based Information Security Analysor (CBISA). Arviointimenetelmien esittelyn jälkeen työssä on vertailtu eri menetelmiä ja todettu, että mikään esitellyistä menetelmistä ei ollut sopiva sellaisenaan. Esitetyt menetelmät olivat joko liian työläitä tai sitten niiden etenemismalli oli sellainen, että prosessin alkuvaiheessa tehty virheellinen arviointi vaikutti läpi koko prosessin vääristäen lopputulosta merkittävästi. Myös liiallinen subjektiivisuus nähtiin ominaisuutena, jota valittavalle menetelmälle ei toivota. Mukana vertailussa oli myös heuristinen menetelmä, jonka antamat lopputulokset arvioitiin hyvin epäluotettaviksi. Työssä on tämän jälkeen kehitetty eri menetelmiä yhdistellen

työkalu, joka täyttää hyvän arviointimenetelmän kriteerit, minkä jälkeen menetelmää on testattu käytännössä, sekä arvioitu menetelmän toimivuutta.

Empiriaosassa on suoritettu valittua menetelmää käyttäen SystemIntelligence Oy:n tietoturva-analyysi. Ensimmäisessä vaiheessa käytiin läpi Finnen mallin mukaiset 12 tietoturvaketjun lenkkiä nelikenttäanalyysin muodossa. Nelikenttätutkimukseen saatiin vastaukset kolmelta eri henkilöltä, joiden vastaukset analysoitiin ja niistä tehtiin yhteenveto. Analyysin ja yhteenvedon tulosten perusteella suoritettiin "rikastaminen", jonka tuloksena analyysin toiseen vaiheeseen valittiin viisi tietoturvallisuuden osa-aluetta.

Toisen vaiheen analyysin johtopäätöksenä on todettu, että kohdeyrityksen tietoturvallisuuden taso on jatkuvasti heikkenemässä liiketoiminnan kasvun myötä. Nykyiset toimenpiteet eivät enää ole riittäviä tulevaisuuden toimintaympäristössä. Henkilökunnan määrän kasvaessa tulee henkilöstöturvallisuuteen kiinnittää enemmän huomiota, lisätä tietoturvakulttuurin merkitystä, sekä muuttaa toimintatapoja jokapäiväisessä toiminnassa. Jatkossa on myös syytä vastuuttaa tietoturva-asiat tätä varten osoitetulle henkilölle, jolla tulisi myös olla valtuudet ja resurssit vastata koko yrityksen hallinnollisesta tietoturvasta.

Tässä työssä kehitetyn mallin tarkoituksena oli olla riittävän yksinkertainen ja kevyt toteuttaa. Tarkoitus oli löytää menetelmä, jolla yksiselitteisesti voidaan erottaa tietoturvakokonaisuudesta ne osa-alueet, joiden jatkokäsittely on aiheellista. Tässä vaiheessa tulisi voida jättää sivuun ne osa-alueet, jotka eivät käsiteltävän yrityksen kannalta ole merkittäviä joko niiden epätodennäköisyyden tai pienen taloudellisen merkityksen vuoksi.

Analyysin ensimmäisessä vaiheessa kyselyyn osallistuneet henkilöt sijoittivat omat vastauksensa nelikenttään, jonka x-(vahingon suuruus) ja y-akseli (tapahtuman todennäköisyys) saivat arvoja ”suuri” ja ”pieni”. Tarkoitus oli alunperin valita jatkokäsittelyyn ne tietoturvaketjun lenkit, jotka saavat molemmilla akseleilla arvon ”suuri” useamman kuin yhden vastaajan nelikentässä. Ensimmäisen vaiheen tuloksena oli kuitenkin vain yksi tietoturvan osa-alue (toimintasuunnitelmat), joka täytti edellä mainitun kriteerin. Karsimalla joukosta ne osa-alueet, jotka puolestaan saivat molempien kriteereiden suhteen arvosanan ”pieni”, saatiin osa-alueiden määrää supistettua, mutta edelleenkään se ei tarjonnut valintakriteeriä toiseen vaiheeseen mukaan otettaville osa-alueille.

Toiseen vaiheeseen valittavien osa-alueiden valintamenetelmää jouduttiin muuttamaan analyysin edetessä siten, että mukaan arviointiin otettiin vastaajien antamat vapaat kommentit, sekä arvioitiin vastaajien tehtävänimikkeen ja toimenkuvan perusteella heidän asennettaan nimenomaisesti hallinnollista tietoturvaa kohtaan. Jako hallinnollisten ja teknisten vastausten välillä oli selkeä, sillä tekniseltä kannalta (= yrityksen oman tuotteen kannalta) tietoturva on hyvällä mallilla, joten tämä selitti useassa kohdassa esiintyneet ristiriitaisuudet eri vastaajien antamien arvosanojen välillä. Laajentamalla valintakriteeriä ja huomioimalla vastaajan oma asema yrityksessä saatiin toiseen vaiheeseen valittua kaikkiaan viisi osa-aluetta, mikä tuntui sopivalta määrältä otettavaksi mukaan jatkoanalyysiin.

- Toimintasuunnitelmat (suuri, suuri)
- Tietokoneturvallisuus (pieni, suuri)
- Henkilöstöturvallisuus (pieni, suuri)
- Ulkoiset ja sisäiset uhkatekijät (suuri, pieni)
- Asenteet tietoturvaa kohtaan (suuri, pieni)

Toisessa vaiheessa käytiin valitut tietoturvaketjun lenkit läpi Finnen esittämän jaottelun mukaisesti. Osa Finnen mallin osa-alueista oli ainakin valitun yrityksen kannalta täysin epärelevantteja ja siksi ne ohitettiin maininnalla. Merkitykselliset kohdat käsiteltiin tarkemmin. Analyysin tuloksena löytyikin suurehko joukko seikkoja, jotka eivät tänä päivänä kohdeyrityksessä vastaa hyvää tietoturvan tasoa. Näiden seikkojen suhteen on työssä esitetty toimenpide-ehdotuksia.

Työssä kehitetyn mallin toimivuus ei ollut aivan toivottua luokkaa. Suurimmaksi ongelmaksi analyysissa osoittautui valinnan suorittaminen nelikentän vastausten pohjalta. Vastausten hajonta oli odotettua suurempi, joten jatkoanalyysiin valinta jouduttiin osittain suorittamaan käyttäen muuta kriteeristöä kuin mitä oli alunperin mallissa ajateltu.

Toisen vaiheen valinnan jälkeen Finnen malli tuntui soveltuvan melko hyvin jatkotyöskentelyyn. Oman problematiikkansa analyysiin aiheutti se, että osa Finnen määrittelemistä osa-alueista on jo vanhentunutta teknologiaa, joka ei tänä päivänä ole relevanttia. Tässä työssä pyrittiin ohittamaan lyhyesti vanhentuneet menetelmät ja keskittymään niihin, joilla on merkitystä.

Analyysin lopputuloksena oli joukko asioita, joita kohdeyrityksessä tulisi kehittää, sekä toimenpidesuosituksia asioiden korjaamiseksi. Arvion mukaan mallin avulla löydettiin kohdeyrityksen kannalta merkittävimmät tietoturva-aukot, sekä keinot niiden paikkaamiseksi. Tältä osin valittu malli siis tuotti toivotun lopputuloksen. Jatkotutkimuksia varten valittua mallia tulisi todennäköisesti kuitenkin kehittää jonkin verran, jotta ensimmäisen vaiheen jälkeinen karsinta tapahtuisi ilman tarkentavia taustatietoja vastaajista.

Yhteenvetona mallin toimivuudesta voidaan todeta, että varmaa tietoa sen toimivuudesta ei tämän yksittäisen analyysin pohjalta ole olemassa, vaan sitä tulisi jatkossa testata useammassa kohdeyrityksessä. Nyt tehty analyysi antaa kuitenkin viitauksia siihen, että kehitetty nelikenttä sulkee liian tiukasti pois analysoitavia osa-alueita, mikäli kyselyyn vastanneiden henkilöiden joukko on liian heterogeeninen. Koska heterogeeninen vastaajajoukko antaa kuitenkin monipuolisemman kuvan tutkittavan yrityksen tilanteesta kuin homogeenisempi joukko, näyttäisi järkevältä laajentaa toisessa vaiheessa tutkittavien osa-alueiden kriteerejä. Tämä tulisi kuitenkin tehdä siten, että tutkittavasta joukosta ei tule jatkossa liian suuri.

LÄHDELUETTELO

KIRJALLISET LÄHTEET

Daler, Torgeir & Gulbrandsen, Roar & Melgård, Birger & Sjolstad, Torbjor. 1989. *Security of Information and Data.* Ellis Horwood Limited, Halsted Press: a division of John Wiley & Sons.

Elbra, R.A. 1992. *Computer Security Handbook.* NCC Blackwell Limited, England.

Ernst & Young.2004. Global Information Security Survey 2004.

Finne, Thomas. 1996. *Analysing Information Security: A Knowledge-based DSS Approach.* Meddelanden från ekonomisk-statsvetenskapliga fakulteten vid Åbo Akademi, Institute for Advanced Management Systems Research Ser.A:456. Åbo Akademis tryckeri, Åbo.

Finne, Thomas.1998. *A Decision Support System for Improving Information Security.*Turku Centre for Computer Science TUCS Dissertations No 8. Painosalama Oy, Turku.

Fisher, Royal P. 1984. *Information Systems Security.* Prentice-Hall Inc., New Jersey.

Freese Jan & Holmberg Sten. 1988. *Data Osäkerhet; Praktisk Handbok för Beslutsfattare.* Affärsinformation AB, Stockholm och Universitetsforlaget A/S, Norbok A/S, Norge.

Gollman, Dieter. 1999. *Computer Security*. Third Edition. John Wiley & Sons Ltd, West Sussex, England.

Hannula Antti & Siilasmaa Risto. 1991. *Mikrojen tietoturva*. Datacasa & Datafellows, Gummerus kirjapaino Oy, Jyväskylä.

Kyrölä Tuija. 2001. *Esimies ja tietoriskien hallinta*. WS Bookwell Oy, Juva.

Lane V.P. 1985. *Security of Computer Based Information Systems*. Macmillan Education Ltd, Camelot Press Ltd, Southampton, England.

Ledell & Roman & Voutilainen. 1985. *Tietosuojaopas –mirkotietokoneiden käyttäjille*, Proteva Security ja Amersoft, Mäntän kirjapaino Oy, Mänttä.

Lujanen, Pentti (toim). 1991. *Yrityksen tietoturva*. Suomen Atk-kustannus Oy, Myllykoski.

Market-Visio Oy. 2002. *Tietoturva – uhat, suojautuminen ja markkinanäkymät 2002 – 2004.*

Porvari Paavo (toim). 1994. *Tietoturvallisuuden tason arviointi*. Pohjola-yhtiöiden julkaisuja 18.

PriceWaterhouse. 1990. *The Complete Computer Virus Handbook*. Second Edition. Pitman Publishing, London, England.

PriceWaterhouseCoopers. 2002. *Information Security Breaches Survey (ISBS) 2002.*

Saarenpää Ahti & Pöysti Tuomas & Sarja Mikko & Still Viveca & Balboa-Alcoreza Ruxandra. 1997. *Tietoturvallisuus ja laki, Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä.* Tutkimusraportti, Valtiovarainministeriö, Hallinnon kehittämisosasto, Lapin yliopiston oikeusinformatiikan instituutti. Edita Oy.

Salminen, Helvi (toim).1997. *Tietoturvallisuus etätyössä.* Suomen Atk-kustannus Oy. Gummerus Kirjapaino Oy, Jyväskylä.

Siponen, Mikko. 2002. *Designing Secure Information Systems and Software, Critical evaluation of the existing approaches and a new paradigm.* Department of Information Processing Science and Infotech Oulu, University of Oulu.

Tarkoma, Jarno. 1998. *Toinen Internet: Riskit, rikkeet ja verkkokaupankäynti.*Taloustieto Oy, Tammer-Paino Oy, Tampere.

Tietojärjestelmien tarkastus ja valvonta ry. 1997. *Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja.* Suomen Atk-kustannus Oy, Gummerus Kirjapaino Oy, Jyväskylä.

Turban Efraim & McLean Ephraim & Wetherbe James. 1999. *Information Technology for Management, Making Connections for Strategic Advantage.* 2nd Edition. John Wiley & Sons,Inc.

HAASTATTELUT

Software Engineer. SystemIntelligence Oy, Helsinki. 15.03.2005.

Software Developer. SystemIntelligence Oy, Helsinki.17.03.2005.

PROBABILITY RANGE TABLE

Subjective Frequency Time	Value (P)	Annualized Per Year	Loss Multiplier (PL)
Once in 300 years	1	1 / 300	0,00333
Once in 30 years	2	1 / 30	0,03333
Once in 3 years	3	1 / 3	0,33333
Once in 100 days	4	365 / 100	3,65
Once in 10 days	5	365 / 10	36,5
Once per day	6	365 / 1	365
10 times per day	7	365 / 0,1	3650
100 times per day	8	365 / 0,01	36500

Lähde: Fisher 1984, 85

COST / LOSS RANGE TABLE

Subjective Cost ($)	Constant Value (C)
0 - 10	1
10 - 100	2
100 - 1K	3
1K - 10K	4
10K - 100K	5
100K - 1M	6
1M - 10M	7
10M - 100M	8

Lähde: Fisher 1984, 87

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

SAATTEEKSI TIETOTURVAKYSELYYN

Mistä on kyse?

Olen Tuula Laukkarinen ja aloitan työskentelyn SystemIntelligence Oy:ssä Finance Directorina 11.1.2005.

Ennen töiden alkua pidän pienen opintovapaan, jonka aikana toivon saavani Pro Gradu – tutkielmaani edistettyä. Teen gradua HKKK:n tietojärjestelmätieteen laitokselle ja aiheenani on Pk –yrityksen tietoturva. Tätä tarkoitusta varten olen saanut SystemIntelligence Oy:n toimitusjohtajalta luvan vaivata muutamia SystemIntelligencen työntekijöitä pyytämällä heitä vastaamaan oheiseen kyselyyn. Toivon, että Sinulta löytyisi aikaa vastata tähän pikaisesti, jotta pääsisin jatkojalostamaan kyselyn tuloksia.

Palautatko kyselyn Office Managerille, joka ystävällisesti on lupautunut välittämään kyselylomakkeet sekä valitsemaan henkilöstön joukosta kyselyyn osallistuvat.
Mikäli haluat kysyä jotain tähän tutkimukseen liittyen, minut tavoitat kännykästä 050-5114580 tai sähköpostilla osoitteesta tupu_la@suomi24.fi.

Kiitokseni jo etukäteen vaivannäöstäsi!

t.tupu

Ohjeet

Alla on tietoturva jaettu 12 osa-alueeseen. Jokaisesta osa-alueesta on joitain kysymyksiä kyselyyn vastaajan johdattamiseksi oikeaan asiaan. Lue kunkin osa-alueen kysymykset ennen vastaamista. Muodostettuasi mielipiteesi kyseisestä osa-alueesta, sijoita osa-aluetta vastaava numero (1 – 12) oheiseen nelikenttään siihen ruutuun, joka mielestäsi parhaiten vastaa SystemIntelligence Oy:n tämän hetkistä tilannetta kyseisen osa-alueen suhteen.

Laita vielä lyhyt perustelu / kommentti asioista, jotka vaikuttivat kyseisen kohdan vastaukseen. Jos jokin asia on mielestäsi huonosti / hyvin hoidettu, laita perustelusi yhdellä lauseella.

Saisinko vielä nimesi tähän paperiin, jonka toivon myös palautettavan, jotta osaan yhdistää saman vastaajan kommentit ja nelikentän toisiinsa.

Nimi:_____

Käytän kommentteja vain mahdollisten lisäkysymysten tekemiseen, mikäli sellaisiin on tarvetta.

Nyt itse asiaan....

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

Tietoturvan osa-alueet

1. Tietokoneturvallisuus (Computer security)
   - pidetäänkö yrityksessäsi varmuuskopiointia tärkeänä?
   - käytetäänkö yrityksessäsi viruksentorjuntaohjelmistoja?
   - kryptataanko yrityksessäsi dataa?
   - onko salasanoilla minimipituus?
   - onko salasanat pakko vaihtaa tietyin väliajoin?
   -

2. Toiminnan turvallisuus (Operation security)
   - testataanko ohjelmistot ennen käyttöönottoa?
   - onko käyttäjätunnusten käyttö tärkeää?
   - seurataanko lokitiedostoja?
   - voivatko ulkopuoliset päästä käsiksi yrityksen tiedostoihin?
   -

3. Varkauksilta suojautuminen (Protection against burglary)
   - onko varkauksilta suojautuminen tärkeää?
   - ovatko laitteet kiinnitettyinä esim. toimistokalusteisiin?
   - käytetäänkö kulunvalvontaa?
   - onko laitteisto turvamerkittyä?
   - ovatko kannettavat työasemat lukittuja?
   -

4. Tulipalolta suojautuminen (Protection against fire)
   - onko yrityksessäsi palohälyttimet?
   - onko sprinklereitä?
   - onko käytössä datakaappeja, joiden palonkestävyys on luokiteltu?
   - ovatko varmuuskopiot samassa laitetilassa esim. palvelinten kanssa?
   -

5. Vesivahingolta suojautuminen (Protection against water damage)
   - ovatko yrityksen rakenteet veden kestäviä?
   - onko käytössä vesitunnistimia?
   - onko tietovälineet suojattu vedeltä riittävästi?
   -

6. Virranjakelun varmistaminen (Electricity distribution)
   - onko käytössä UPSit?
   - kauanko virranjakelun keskeytys voi jatkua ilman mittavia häiriöitä yrityksen toiminnalle?
   - ovatko elektromagneettiset häiriöt mahdollisia?

7. Ulkoiset ja sisäiset uhkatekijät (Extern and internal threats)
   - onko sabotaasi mahdollista?
   - onko vakoilun uhka todellinen?
   -

8. Tietoliikenne (Communication)
   - ovatko puhelinlinjat suojattuja?
   - käytetäänkö takaisinsoittomodeemeja?
   - onko nettikäyttöä rajattu?
   - onko yrityksessäsi palomuuri?
   - onko etäyhteydet suojattu?
   -

9. Toimintasuunnitelmat (Contingency planning)
   - onko olemassa toipumissuunnitelma?
   - onko varajärjestelmiä testattu?
   - kauanko varmuuskopioiden palauttaminen kestää?
   - saako kaupasta varaosia laitteisiin?
   - onko yhteensopivia laitteita vielä kaupan, jos nykyisiä laitteita vahingoittuu?
   -

10. Henkilöstöturvallisuus (Personnel security)
    - onko henkilöstöturvallisuus tärkeää yrityksessäsi?
    - tarkistetaanko uuden työntekijän taustoja?
    - onko irtisanoutuneen / irtisanotun työntekijän aiheuttamista toimenpiteistä turvaohjetta?
    - onko vierailijoita varten turvaohjeet?
    - onko yrityksessäsi järjestetty tietoturvakoulutusta?
    - onko yrityksessäsi nimetty tietoturvapäällikkö?
    -

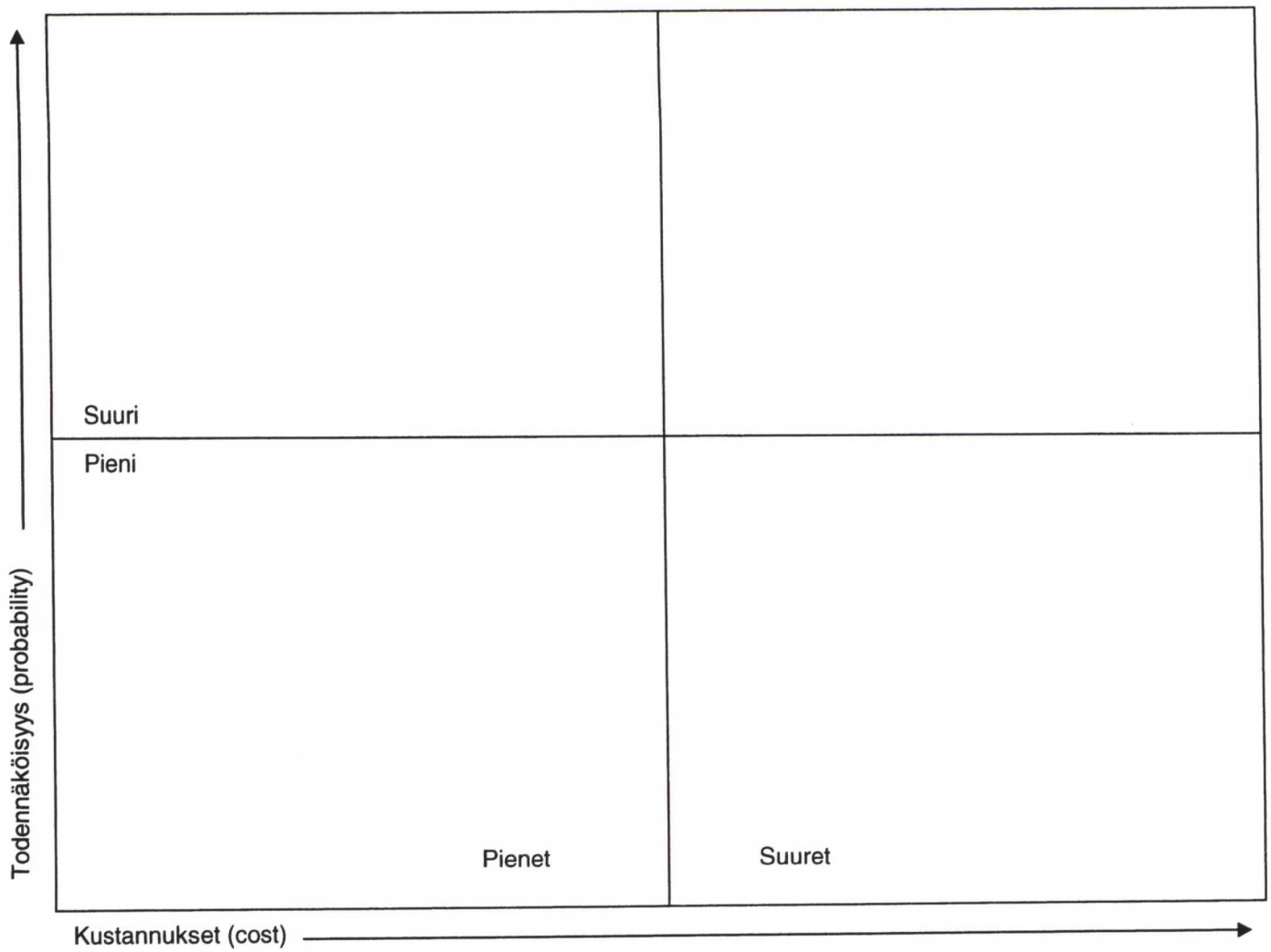
11. Asenteet tietoturvaa kohtaan (Attitudes towards security issues)
    - onko olemassa kirjallinen tietoturvapolicy?
    - onko olemassa tietoturvakulttuuri?
    - onko tietoturvarikkomuksista määritelty sanktioita?
    -

12. Muut turvallisuusasiat (Various security questions)
    - onko paperitulosteiden käsittelystä erityisohjeita (esim. tietoturvaluokitukset)?
    - onko erilliset tietoturvaroskikset?
    - onko kiinteistöturvallisuus kunnossa?
    - kosteuden, lämpötilan, pölyn ym. vaikutukset tietovälineisiin?
    - sähköpostien käsittely?
    - muun postin käsittely (esim. kuka avaa postin)?
    -

Nimi

Asema yrityksessä

Päivämäärä



Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

Tietoturvan osa-alueet

1. Tietokoneturvallisuus (Computer security)
   - pidetäänkö yrityksessäsi varmuuskopiointia tärkeänä? Pidetään, muttei varmuuskopioida riittävästi
   - käytetäänkö yrityksessäsi viruksentorjuntaohjelmistoja? Kyllä
   - kryptataanko yrityksessäsi dataa? Kannettavien tietokoneiden tiedot pitäisi vähintään kryptata, mutta niin ei yleisesti tehdä.
   - onko salasanoilla minimipituus? Ei, ohjeistukset tähän on kyllä jaettu.
   - onko salasanat pakko vaihtaa tietyin väliajoin? Ei, mutta tietokoneethan ehdottavat/vanhentavat salasanat, ja sitä kautta ne on vaihdettava. Tämä ei siis estä kuitenkaan saman salasanan käyttämistä yhä uudelleen.
   -

2. Toiminnan turvallisuus (Operation security)
   - testataanko ohjelmistot ennen käyttöönottoa? Siis mikäli tarkoitat valmistamaamme tuotetta, niin testataan. Mikäli tarkoitat yleisiä ohjelmistoja esim. MS Windows, niin käsittääkseni ladataan suoraan koneelle.
   - onko käyttäjätunnusten käyttö tärkeää? Käyttäjätunnukset ovat käytössä, ja niiden seuranta myös tärkeää (erityisesti **omassa** tuotteessa)
   - seurataanko lokitiedostoja? Ei kuulemma erityisesti seurata, vaikka mahdollisuus tähän toki on.
   - voivatko ulkopuoliset päästä käsiksi yrityksen tiedostoihin? Käsittääkseni ei. Yrityksen sisällä on palomuuri, ja palomuurit ovat myös kannettavissa tietokoneissa (etätyö).
   -

3. Varkauksilta suojautuminen (Protection against burglary)
   - onko varkauksilta suojautuminen tärkeää? Kannettavailla tietokoneilla on erittäin tärkeitä tietoja, kuten myös toimistossa. Suojautuminen on siis erittäin tärkeää.
   - ovatko laitteet kiinnitettyinä esim. toimistokalusteisiin? Ei ole. Messuilla ym. Kannettavat koneet lukitaan kiinni kalusteisiin.
   - käytetäänkö kulunvalvontaa? Kyllä. (Toimistotiloihin kuljetaan kahden lukitun oven kautta, jotka aukeavat tunnisteavaimella)
   - onko laitteisto turvamerkittyä? Ei ole.
   - ovatko kannettavat työasemat lukittuja? Kannettavat työasemat voidaan lukita, mutta harvoin ovat lukitussa tilassa.
   -

4. Tulipalolta suojautuminen (Protection against fire)
   - onko yrityksessäsi palohälyttimet? Palohälyttimet on käsittääkseni koko kiinteistössä
   - onko sprinklereitä? On.
   - onko käytössä datakaappeja, joiden palonkestävyys on luokiteltu? Ei ole palonkestäviä arkistokaappeja.

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

- ovatko varmuuskopiot samassa laitetilassa esim. palvelinten kanssa? Ennen ei, nykyään en tiedä, mutta tuskin on.
-

5. Vesivahingolta suojautuminen (Protection against water damage)
   - ovatko yrityksen rakenteet veden kestäviä? Missä mielessä? Luulisin, että ei.
   - onko käytössä vesitunnistimia? Ei
   - onko tietovälineet suojattu vedeltä riittävästi? Kyllä.
   -
6. Virranjakelun varmistaminen (Electricity distribution)
   - onko käytössä UPSit? Varavoimanlähteitä ei ole omassa käytössä. Amerilla saattaa olla jonkinlainen, lähinnä kai omien kriittisten tietojen saamisen takaamiseksi.
   - kauanko virranjakelun keskeytys voi jatkua ilman mittavia häiriöitä yrityksen toiminnalle? Todella vähän aikaa.
   - ovatko elektromagneettiset häiriöt mahdollisia? On teoriassa, käytännössä ei. Sähkövarausta on joka paikassa.

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

7. Ulkoiset ja sisäiset uhkatekijät (Extern and internal threats)
   - onko sabotaasi mahdollista? ?
   - onko vakoilun uhka todellinen? On. Tuote on lähdekoodi muodossa.
   -

8. Tietoliikenne (Communication)
   - ovatko puhelinlinjat suojattuja? Ei
   - käytetäänkö takaisinsoittomodeemeja? Ei, mahdollisesti tuotekehityksen puolella.
   - onko nettikäyttöä rajattu? Ei
   - onko yrityksessäsi palomuuri? On
   - onko etäyhteydet suojattu? Ei/ On, palomuurit on kannettavissa koneissa.
   -

9. Toimintasuunnitelmat (Contingency planning)
   - onko olemassa toipumissuunnitelma? Ei
   - onko varajärjestelmiä testattu? Ei ole varajärjestelmää
   - kauanko varmuuskopioiden palauttaminen kestää? ?
   - saako kaupasta varaosia laitteisiin? Saa, muttei kannata yleensä ostaa, kun uuden koneen hankinta tulee samanhintaiseksi.
   - onko yhteensopivia laitteita vielä kaupan, jos nykyisiä laitteita vahingoittuu? Juu ja ei
   -

10. Henkilöstöturvallisuus (Personnel security)
    - onko henkilöstöturvallisuus tärkeää yrityksessäsi? On
    - tarkistetaanko uuden työntekijän taustoja? Ei
    - onko irtisanoutuneen / irtisanotun työntekijän aiheuttamista toimenpiteistä turvaohjetta? On ohjeet lähtevälle työntekijälle, muttei ohjetta siltä varalta, että lähtenyt aiheuttaa yritykselle lähdön jälkeen vahinkoa.
    - onko vierailijoita varten turvaohjeet? Mikäli tarkoitat tietoturvallisuusohjeita niin on. Vierailijat ohjataan ovea lähimpänä olevaan neuvottelutilaan, eikä vieraat käytännössä käy muissa yrityksen tiloissa.
    - onko yrityksessäsi järjestetty tietoturvakoulutusta? Ei
    - onko yrityksessäsi nimetty tietoturvapäällikkö? Ei
    -

11. Asenteet tietoturvaa kohtaan (Attitudes towards security issues)
    - onko olemassa kirjallinen tietoturvapolicy? Ei
    - onko olemassa tietoturvakulttuuri? Ei varsinaista, mutta on kuitenkin
    - onko tietoturvarikkomuksista määritelty sanktioita? Ei
    -

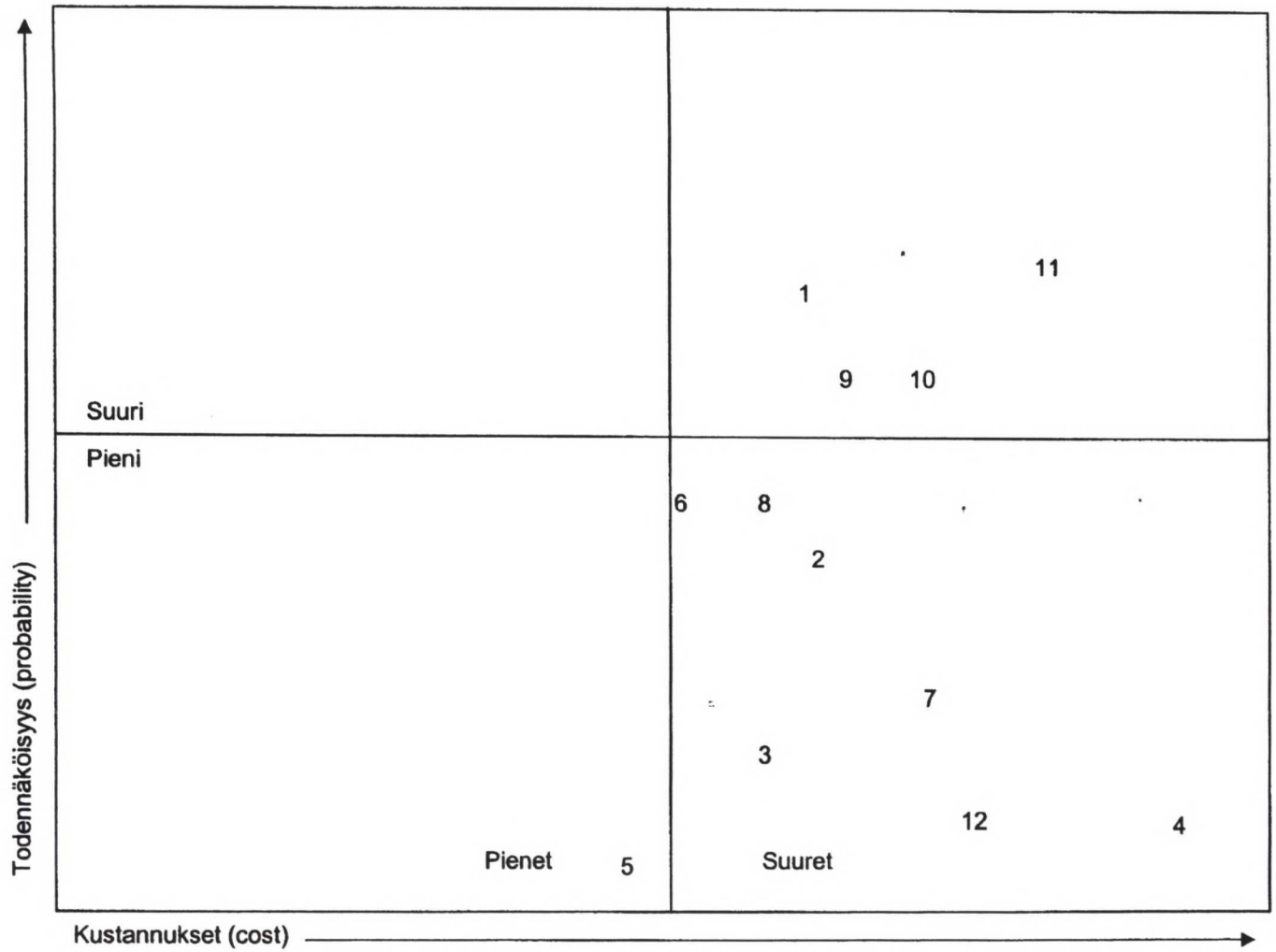
12. Muut turvallisuusasiat (Various security questions)
    - onko paperitulosteiden käsittelystä erityisohjeita (esim. tietoturvaluokitukset)? Luottamuksellinen tieto silppurin läpi.
    - onko erilliset tietoturvaroskikset? On, silppuri
    - onko kiinteistöturvallisuus kunnossa? On

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

- kosteuden, lämpötilan, pölyn ym. vaikutukset tietovälineisiin? Ei haittavaikutuksia => siivoojien ohjeet pölyn poistamiseksi. Serverit säilytetään kellarissa viileämmissä tiloissa.
- sähköpostien käsittely? On ok.
- muun postin käsittely (esim. kuka avaa postin)? Posti nimetyille henkilöille. Muun postin avaa toimistopäällikkö
-
-

Asema yrityksessä **Office Manager, SystemIntelligence Oy**

Päivämäärä 10.12.2004



Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

Tietoturvan osa-alueet

1. Tietokoneturvallisuus (Computer security)
   - pidetäänkö yrityksessäsi varmuuskopiointia tärkeänä? Kyllä. Päivittäiset
   - käytetäänkö yrityksessäsi viruksentorjuntaohjelmistoja? Kyllä (vain Windows + email)
   - kryptataanko yrityksessäsi dataa? Käytännössä ei, siirron aikana aina
   - onko salasanoilla minimipituus? O.v (vaihtelee systeemeittäin)
   - onko salasanat pakko vaihtaa tietyin väliajoin? Ei (se heikentäisi tietoturvaa)
   -

2. Toiminnan turvallisuus (Operation security)
   - testataanko ohjelmistot ennen käyttöönottoa? K.
   - onko käyttäjätunnusten käyttö tärkeää? K
   - seurataanko lokitiedostoja? Osan
   - voivatko ulkopuoliset päästä käsiksi yrityksen tiedostoihin? Ei ilman noaita
   -

3. Varkauksilta suojautuminen (Protection against burglary)
   - onko varkauksilta suojautuminen tärkeää? K
   - ovatko laitteet kiinnitettyinä esim. toimistokalusteisiin? Ei "
   - käytetäänkö kulunvalvontaa? K
   - onko laitteisto turvamerkittyä? Ei
   - ovatko kannettavat työasemat lukittuja? Ei
   -

4. Tulipalolta suojautuminen (Protection against fire)
   - onko yrityksessäsi palohälyttimet? Kyllä
   - onko sprinklereitä? Valitettavasti
   - onko käytössä datakaappeja, joiden palonkestävyys on luokiteltu? Paimolla tiitaa olla
   - ovatko varmuuskopiot samassa laitetilassa esim. palvelinten kanssa? Riippuu palvelusta. Osa o.v
   -

5. Vesivahingolta suojautuminen (Protection against water damage)
   - ovatko yrityksen rakenteet veden kestäviä? E
   - onko käytössä vesitunnistimia? E
   - onko tietovälineet suojattu vedeltä riittävästi? E
   -

6. Virranjakelun varmistaminen (Electricity distribution)
   - onko käytössä UPSit? Kyllä
   - kauanko virranjakelun keskeytys voi jatkua ilman mittavia häiriöitä yrityksen toiminnalle? Puolisen tuntia (ilman talun omaa varavoimaa)
   - ovatko elektromagneettiset häiriöt mahdollisia? Ei

Tuula Laukkarinen
HKKK / Tietojärjestelmätiede

7. Ulkoiset ja sisäiset uhkatekijät (Extern and internal threats)
   - onko sabotaasi mahdollista?
   - onko vakoilun uhka todellinen? ON, KOODI ON AVOINTA
   -

8. Tietoliikenne (Communication)
   - ovatko puhelinlinjat suojattuja? EI
   - käytetäänkö takaisinsoittomodeemeja? EI
   - onko nettikäyttöä rajattu? EI
   - onko yrityksessäsi palomuuri? KYLLÄ
   - onko etäyhteydet suojattu? KYLLÄ (EI VPN:LLÄ, ONNEKSI)
   -

9. Toimintasuunnitelmat (Contingency planning)
   - onko olemassa toipumissuunnitelma? EI TIETOA
   - onko varajärjestelmiä testattu? EI
   - kauanko varmuuskopioiden palauttaminen kestää? MUUTAMAN TUNNIN
   - saako kaupasta varaosia laitteisiin? KYLLÄ
   - onko yhteensopivia laitteita vielä kaupan, jos nykyisiä laitteita vahingoittuu? KYLLÄ
   -

10. Henkilöstöturvallisuus (Personnel security)
    - onko henkilöstöturvallisuus tärkeää yrityksessäsi?
    - tarkistetaanko uuden työntekijän taustoja? EI TIETOA
    - onko irtisanoutuneen / irtisanotun työntekijän aiheuttamista toimenpiteistä turvaohjetta? OSITTAIN
    - onko vierailijoita varten turvaohjeet? EI
    - onko yrityksessäsi järjestetty tietoturvakoulutusta? EI
    - onko yrityksessäsi nimetty tietoturvapäällikkö? EI
    -

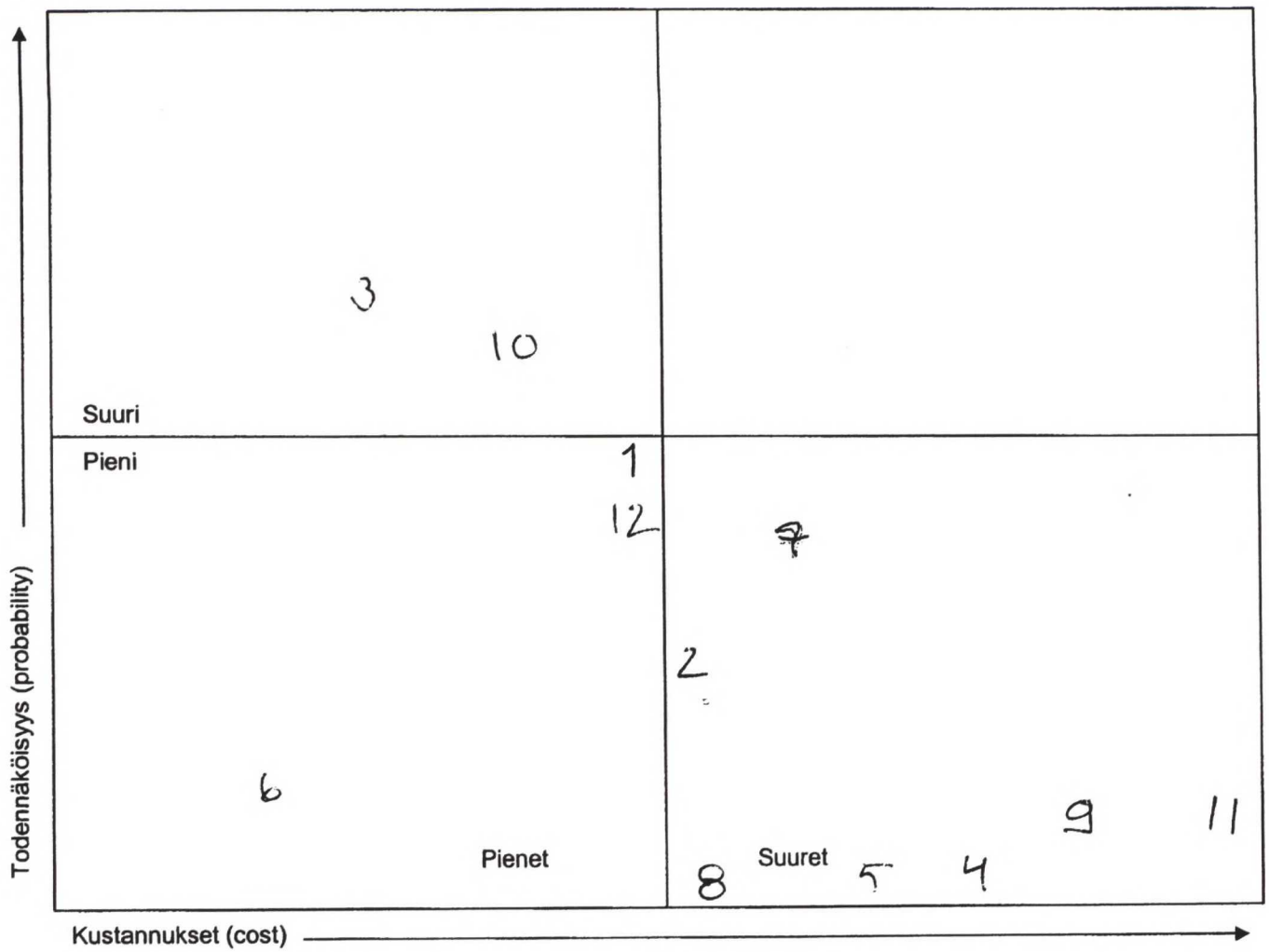
11. Asenteet tietoturvaa kohtaan (Attitudes towards security issues)
    - onko olemassa kirjallinen tietoturvapolicy? EI
    - onko olemassa tietoturvakulttuuri? KYLLÄ
    - onko tietoturvarikkomuksista määritelty sanktioita? LAKI MÄÄRITTELEE
    -

12. Muut turvallisuusasiat (Various security questions)
    - onko paperitulosteiden käsittelystä erityisohjeita (esim. tietoturvaluokitukset)?
    - onko erilliset tietoturvaroskikset? SILPPURI LUKITAAN
    - onko kiinteistöturvallisuus kunnossa? K
    - kosteuden, lämpötilan, pölyn ym. vaikutukset tietovälineisiin? EI SUORITTAA
    - sähköpostien käsittely? ?
    - muun postin käsittely (esim. kuka avaa postin)? OFFICE MANAGER TAI TOIMITUSJOHTAJA
    -

Nimi

Asema yrityksessä Software Engineer, SystemIntelligence Oy

Päivämäärä 10.12.2004

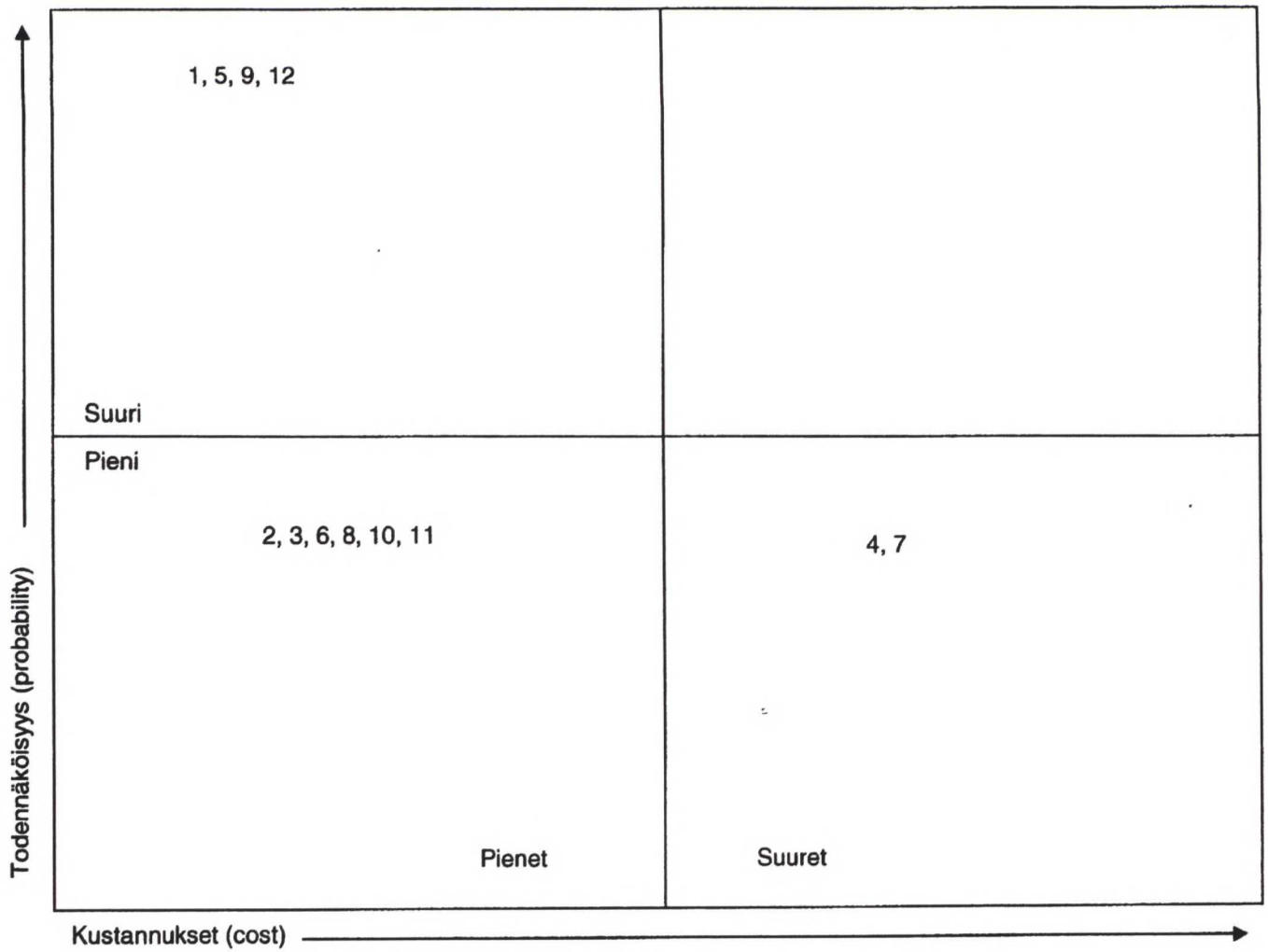


Asema Yrityksessä: Product Architect

>Subject: Vastauksia tietoturvakyselyyn
>
>1. tietokoneturvallisuus
> - kannettavien koneiden tietoja ei suojattu varkauksilta
> - tiedot pääasiassa omassa järjestelmässä (hallinnointi ulkoistettu) sekä käyttäjien
>työasemilla. työasemat ei varmistettuja.
> - salasanoille ei rajoituksia eikä vaihtopakkoa
> ==> 1
>
>2. toiminnan turvallisuus
> ==> 3
>
>3. varkauksilta suojautuminen
> - palvelimet erillisessä huoneessa
> - kulunvalvonta käytössä
> ==> 3
>
>4. tulipalolta suojautuminen
> - varmuuskopionauhoja viety satunnaisesti tallelokeroon
> ==> 2
>
>5. vesivahingolta suojautuminen
> ==> 1
>
>6. virranjakelun varmistaminen
> - UPSeista riittää virtaa noin 30-60min
> - palvelimia ei asetettu ajamaan alas virran loppuessa
> - työasemilla ei varavirtaa
> ==> 3
>
>7. ulkoiset ja sisäiset uhkatekijät
> ==> 4
>
>8. tietoliikenne
> - nettikäyttö ei rajoitettu, palomuuri olemassa
> - etäyhteydet suojattuja sähköpostia ja kalenteria lukuunottamatta
> ==> 3
>
>9. toimintasuunnitelmat
> - operatiiviset tietojärjestelmät ulkoistettu kalenteria
>lukuunottamatta
> - tuotekehityksen koneet itse hallinnoituja
> ==> 1
>
>10. henkilöstöturvallisuus
> ==> 3
>
>11. asenteet tietoturvaa kohtaan
> - ei tietoturvakäytäntöä, ei määriteltyjä sanktioita
> ==> 3
>
>12. muut turvallisuusasiat
> - ei käsittelyohjeita, silppuri käytössä
> ==> 1

Product architect

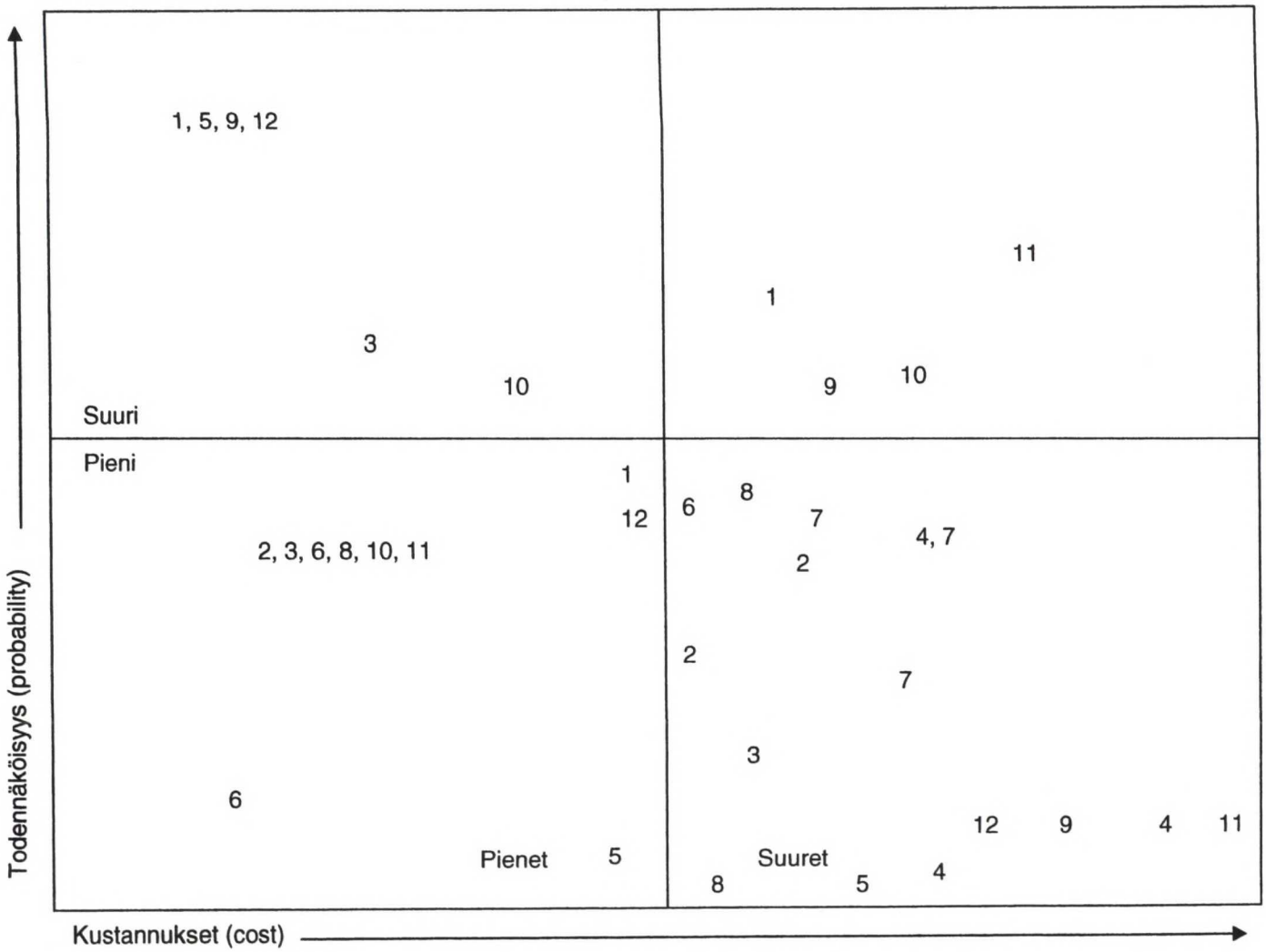
2004-12-10



Nimi: **Yhteenveto**

Asema yrityksessä

Päivämäärä



LIITE 4